UNCLASSIFIED

AR-006-955

AD-A259 969

ELECTRONICS RESEARCH LABORATORY

Information Technology Division

DTIC ELECTE JAN 27 1993 S E D

RESEARCH REPORT
ERL-0621-RR

TECHNICAL RATIONALE FOR AUSTRALIAN COMPUTER SECURITY RISK ANALYSIS GUIDELINES

by

James Hellewell*, Mark Anderson, Brian Billard

* Under contract from AWA Defence Industries

SUMMARY

This document provides guidance to Australian Government agencies, both defence and civilian, on the specification and selection of trusted computing systems and products to be used for the electronic processing of National Security and/or Sensitive Material.

93-01456

JUN 92

COPY No.

APPROVED FOR PUBLIC RELEASE

POSTAL ADDRESS: Director, Electronics Research Laboratory, PO Box 1500, Salisbury, South Australia, 5108.

ERL-0621-RR

UNCLASSIFIED

FOREWORD

Governments at all levels in Australia increasingly are required to hold on their computer systems significant volumes of information that is classified. Given the increasing demand for the connectivity of those systems, it is quite clear that computer security assessment guidelines for managers, tailored to the Australian scene, are necessary to ensure a consistent and, as much as possible, standardised level of security to protect the information they hold.

The guidelines presented herein are designed to give assistance to managers in assessment of the minimum level of trust, and some advice on required functionality, for computing systems which may hold national security or civilian sensitive data. The advice regarding the levels of trust and functionality is presented in the notation specified in the harmonised European Information Technology Security Evaluation Criteria (ITSEC). The guidelines focus on confidentiality and do not explicitly address integrity and availability issues. As yet, the research community has not settled on a definition of integrity and availability, and so it would be premature to propose minimum standards with respect to those two security requirements.

The guidelines are based on an enumeration of threat environments and quantitative risk analysis and can show correspondence to the US National Computer Security Center (NCSC) standard, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" (Yellow Book) as well as the UK DADPSWG/88-1 guidelines. Discussions with various national authorities leads us to believe that the use of other risk methodologies, such as those represented by annual loss estimates and fault tree analyses, are inappropriate for the military domain for several reasons. Prevalent among these is the influence that the subjective opinion of the analyst conducting the risk analysis has on the results. Further, the annual loss estimate model is difficult to apply in a national security context since it is difficult to measure national security "loss" in the form of dollars.

The Yellow Book promulgated by the NCSC does not have the same susceptibility to subjective opinions. It specifies the minimum level of functionality and assurance required in specific military environments. Hence it would at first seem an ideal candidate for use in the military domain as a standard for enforcing the consistent procurement of trusted systems. However, the Yellow Book measures data exposure risk based only on user clearances and the maximum sensitivity level of data held in the system. The sensitivity lost through this ultra-simplicity means that the options available for minimising the required level of trust in computer components by reducing the technical risk for a given environment, is severely restricted. Moreover, all too often the results obtained indicate that the required level of trust is beyond the ability of the current level of technology. Yet many computer security experts are able to see specific factors whereby the risk could be satisfactorily reduced and thus reasonably allow for a lower required level of trust. In summary, the Yellow Book certainly removes the influence of subjectivity by enumerating and aggregating many factors but the heavy price paid is that a worst case analysis results. Landwehr and Lubbes recognised this and attempted to take more factors into account in their risk methodology for US naval systems. However, application of the Landwehr-Lubbes methodology clearly shows that lowering the risk profile in most cases causes severe restrictions on the operational interface.

The strategy of these guidelines is to show a correspondence with the Yellow Book as a point of origin in a given frame of reference, but to take more factors into account while still ensuring that subjectivity on the part of the analyst using the guidelines cannot have an undue influence. Of course these guidelines do not take into account the number of factors that result from first principle techniques, but they are a step in that direction and are able to prove their "pedigree". Intuitively, one would like to see a series of guidelines developed over a period, each consistent with its predecessor, and taking into account more and more factors which can have significant impacts on the risk profile in the government environment, finally arriving at a methodology which has the flexibility of a first principles analysis but is also traceable in origin to an "ancestral" standard.

CONTENTS

Page No.

FOREWORD . . . iii
1 INTRODUCTION . . . 1
1.1 Scope . . . 1
1.2 Purpose . . . 1
2 BACKGROUND . . . 1
2.1 Requirements of the Guidelines . . . 1
2.2 Existing Risk Analysis Approaches . . . 2
2.2.1 Military-Based Approaches . . . 2
2.2.1.1 Yellow Book . . . 3
2.2.1.2 Landwehr and Lubbes . . . 3
2.2.1.3 DADPSWG/88-1 . . . 4
2.2.1.4 Logicon . . . 5
2.2.1.5 ANSSR . . . 5
2.2.2 Commercial-Based Approaches . . . 5
2.2.2.1 Asset-driven Approaches . . . 6
2.2.2.2 Function-driven Approaches . . . 6
2.2.2.3 Vulnerability-driven Approaches . . . 7
2.2.2.4 Qualitative Approaches . . . 7
2.3 Adopted Approach . . . 7
2.4 COMPUSEC Evaluation Criteria . . . 8
2.5 A Comparison with other military-based approaches . . . 9
2.5.1 Yellow Book Method . . . 11
2.5.2 Landwehr and Lubbes Method . . . 11
2.5.3 Logicon Method . . . 11
2.5.4 ANSSR Method . . . 11
2.5.5 DADPSWG/88-1 Method . . . 11
3 RISK MODEL . . . 13
3.1 Assets . . . 13
3.1.1 Data . . . 13
3.1.1.1 National Security Material . . . 13
3.1.1.2 Sensitive Material . . . 15
3.1.2 Data Attributes . . . 15
3.1.2.1 Data Sensitivity . . . 15
3.1.2.2 Data Separation . . . 16
3.1.2.3 Data Volume . . . 17
3.1.2.4 Data Distribution . . . 17
3.1.2.5 Data Availability . . . 18
3.2 Threats . . . 18
3.2.1 Users . . . 19
3.2.2 User Attributes . . . 20
3.2.2.1 User trustworthiness . . . 20
3.2.2.2 Number of Users . . . 22
3.2.2.3 User Clearance Distribution . . . 22
3.2.2.4 Ability of Users . . . 22

3.3 Vulnerabilities 22
3.3.1 System Attributes 22
3.3.1.1 System architecture 24
3.3.1.2 System distribution 24
3.3.1.3 System management 24
3.3.1.4 External environment 24
3.3.1.5 Remote access 25
3.3.1.6 User Interface 25
3.3.1.6.1 Terminal Interface 25
3.3.1.6.2 Host Interface 26
3.3.1.6.3 Host Services 26
3.3.1.7 Development and operational environment 26
3.3.1.8 Opportunity for User Collusion 27
3.3.1.9 Mode of Operation 28
3.4 Threat Effects (Impacts) 28
3.4.2 Safeguards (Countermeasures) 31
3.5 Risk Factor Hierarchy 32
3.5.1 Data Dependent Factors 32
3.5.1.1 Primary 32
3.5.1.2 Ancillary 32
3.5.2 User Dependent Factors 32
3.5.2.1 Primary 32
3.5.2.2 Ancillary 32
3.5.3 System Dependent Factors 34
3.5.3.1 Environment 34
3.5.3.2 User Interface 34
4 RISK ASSESSMENT 34
4.1 Overview 34
4.2 Identify the User Groups 34
4.3 Perform the Risk Assessment 37
4.3.1 Rating Tables 37
4.3.1.1 Primary Data dependent Factors 37
4.3.1.2 Ancillary Data dependent Factors 39
4.3.1.3 Primary User dependent Factor 41
4.3.1.4 Ancillary User dependent Factors 42
4.3.1.5 System dependent Factors 43
4.3.2 Calculation of the Risk Index 45
4.4 Determine the Overall Risk Index 47
4.5 Rationale for the Assessment Methodology 47
4.5.1 Maximum Data Sensitivity 48
4.5.2 Minimum User Clearance 48
4.5.3 Net Ancillary Factor Adjustment 49
4.5.4 DERI Calculation 50
4.5.5 System Risk Calculation 51
4.5.6 Risk Index 51

5 COMPUTER SECURITY REQUIREMENTS . . . 51
5.1 Functionality . . . 52
5.1.1 Identification and Authentication . . . 52
5.1.2 Access Control . . . 53
5.1.2.1 Support of Roles . . . 53
5.1.2.2 Multilevel Communication Channels . . . 53
5.1.2.3 Mandatory Access Rights . . . 53
5.1.2.4 Mapping of Subjects to Objects . . . 53
5.1.2.5 Multilevel Subjects . . . 53
5.1.3 Audit . . . 54
5.2 Assurance . . . 54
5.3 Rationale for Mappings . . . 54
5.3.1 Functionality . . . 54
5.3.2 Assurance . . . 55
5.4 Limitations of TCSs . . . 55
6 NETWORK CONSIDERATIONS . . . 56
6.1 Introduction . . . 56
6.2 Risk Assessment in IAS Networks . . . 57
6.2.1 Logical Security Zones . . . 60
6.2.2 Zone Partitioning . . . 61
6.2.3 Intra-Zone Connections . . . 61
6.2.3.1 Rules for Intra-zone Connection . . . 62
6.2.3.1.1 Export of Data . . . 62
6.2.3.1.2 Import of Data . . . 62
6.2.3.2 Cascading Problem Heuristic . . . 65
6.2.4 Aggregation Effects Assessment . . . 66
6.2.5 Inter-Zone Connections . . . 67
6.2.5.1 Limited Functionality Security Devices . . . 67
6.2.5.1.1 Data Diode . . . 67
6.2.5.1.2 Classification Integrity Filter . . . 67
6.2.5.1.3 Pre-typer . . . 68
6.2.5.2 Rules for Inter-Zone Connection . . . 68
6.2.5.2.1 General Rules . . . 69
6.2.5.2.2 Functionality devices . . . 69
6.2.5.2.2.1 Data Diode . . . 69
6.2.5.2.2.2 Integrity Filter . . . 70
6.2.5.2.2.3 Pre-typer . . . 72
6.2.5.2.2.4 Manual review . . . 73
6.2.5.2.2.5 Transfer of Data via Removable Media . 74
7 ACKNOWLEDGMENTS . . . 74
8 GLOSSARY . . . 74
9 LIST OF ABBREVIATIONS . . . 79
REFERENCES . . . 81
Appendix A . . . 83
A RISK ASSESSMENT TABLES . . . 83
A.1 Security Parameters . . . 83
A.2 Network Security Tables . . . 85

B ALLIES NATIONAL SECURITY EQUIVALENCE TABLES 87
B.1 Data Classification Levels 87
B.2 User Clearance Levels 87
C MAPPINGS OF ITSEC TO OTHER SECURITY CRITERIA 89
C.1 Relationship between ITSEC and TCSEC 89
C.1.1 Rationale for ITSEC to TCSEC Assurance Criteria Mappings 89
C.2 Relationship between ITSEC and CESG Computer Security Memorandum No 3 89
C.2.1 Rationale for ITSEC to CESG Assurance Criteria Mappings 90
D CASE STUDIES 93
D.1 Sea Surface Surveillance System (S4) 93
D.2 Command Support System (CSS) 99
D.3 Civilian System (DEPT X) 106
D.4 Compartmented System (COMP) 113
D.5 A Network of IAS Components (NET) 117

TABLES

Page No.

2.1 A Comparison of Features offered by the military-based Risk Approaches . . . 10
2.2 Comparison of Risk Assessment Methods between these Guidelines and DADPSWG/88–1 . 12
3.1 Relationship between the Protection level of National Security and Sensitive Material . . . 16
3.2 Levels of Sensitive Material which may be accessed by DSAP cleared Personnel . . . 21
3.3 National Security Material — Impacts . . . 30
3.4 Sensitive Material — Impacts . . . 31
4.1 Rating Scale for Maximum Data Sensitivity — National Security Material . . . 38
4.2 Rating Scale for Maximum Data Sensitivity — Sensitive Material . . . 38
4.3 Rating Scale for Exposure of Categories — National Security . . . 39
4.4 Rating Scale for Volume of Data . . . 40
4.5 Rating Scale for Proportion of Data . . . 41
4.6 Rating Scale for Minimum User Clearance — DSAP . . . 41
4.7 Rating Scale for Maximum Data Sensitivity — PoT . . . 42
4.8 Rating Scale for Number of Users . . . 42
4.9 Rating Scale for the Proportion of Users . . . 43
4.10 Rating Scale for Security Environment . . . 43
4.11 Rating Scale for Terminal Type . . . 44
4.12 Rating Scale for Session Type . . . 44
4.13 Rating Scale for Scope of Utilities . . . 44
4.14 Rating Scale for External Environment . . . 45
4.15 Net Ancillary Factor Adjustment . . . 46
4.16 Data Exposure Risk Index . . . 46
4.17 User Interface Rating . . . 46
4.18 System Risk . . . 47
4.19 Overall Risk Index . . . 47
4.20 Data/User Ancillary Factor Weightings . . . 50
5.1 COMPUSEC Functionality Requirements . . . 52
5.2 COMPUSEC Assurance Requirements . . . 54
6.1 Network Component Evaluation Range Tables — National Security Material . . . 57
6.2 Network Component Evaluation Range Tables — Sensitive Material . . . 59
6.3 Communication Channel Functionality . . . 60
A.1 Security Parameters Record . . . 83
A.2 Risk Assessment Record . . . 84
A.3 Network Security Parameter Table . . . 85
A.4 Inter-zone Data Flow Table . . . 86
B.1 Data Classification Equivalences . . . 87
B.2 User Clearance Equivalences . . . 87
C.1 ITSEC/TCSEC Equivalences . . . 89
C.2 ITSEC/CESG Equivalences . . . 90
D.1 Security Parameters S4 — Limited Yellow Book Assessment . . . 94
D.2 Risk Assessment S4 — Limited Yellow Book Assessment . . . 95
D.3 Security Parameters S4 — Full Assessment with single user group . . . 96
D.4 Risk Assessment S4 — Full Assessment with single user group . . . 97
D.5 Security Parameters S4 — Full Assessment with multiple user groups . . . 98
D.6 Risk Assessment S4 — Full Assessment with multiple user groups . . . 99
D.7 Security Parameters CSS — Limited Yellow Book Assessment . . . 101
D.8 Risk Assessment CSS — Limited Yellow Book Assessment . . . 102
D.9 Security Parameters CSS — Full Assessment with single User Group . . . 103
D.10 Risk Assessment CSS — Full Assessment with single User Group . . . 104
D.11 Security Parameters CSS — Full Assessment with multiple User Groups . . . 105
D.12 Risk Assessment CSS — Full Assessment with multiple User Groups . . . 106
D.13 Security Parameters DEPT X — Full Assessment with single User Group . . . 108
D.14 Risk Assessment DEPT X — Full Assessment with single User Group . . . 109

D.15 Security Parameters DEPT X — Full Assessment with multiple User Groups 110
D.16 Risk Assessment DEPT X — Full Assessment with multiple User Groups 111
D.17 Security Parameters DEPT X — Full Assessment with multiple User Groups 112
D.18 Risk Assessment DEPT X — Full Assessment with multiple User Groups 113
D.19 Security Parameters COMP — Limited Yellow Book Assessment 114
D.20 Risk Assessment COMP — Limited Yellow Book Assessment 115
D.21 Security Parameters COMP — Full Assessment with single User Group 116
D.22 Risk Assessment COMP — Full Assessment with single User Group 117
D.23 Security Parameters NET Example 119
D.24 Risk Assessment NET Example 120
D.25 Minimum Component Evaluation Levels NET Example 121
D.26 Network Security Parameter Table NET Example 122
D.27 Intra-zone connection test — Zone A 124
D.28 Cascade Heuristic — Zone A 124
D.29 Minimum Zone Evaluation Levels NET Example 126
D.30 Inter-zone Data Flow Table 126

FIGURES

Page No.

3.1 Risk Model — Assets 14
3.2 Risk Model — Threats 18
3.3 Risk Model — Users 20
3.4 Risk Model — Vulnerabilities 23
3.5 Risk Model — Threat Effects 29
3.6 Risk Model 33
4.1 Risk Assessment Process 35
4.2 Risk Index Calculation 36
6.1 Intra-zone Connections — Example 1 63
6.2 Intra-zone Connections — Example 2 63
6.3 Intra-zone Connections — Example 3 64
6.4 Intra-zone Connections - Example 4 64
6.5 Intra-zone Connections - Example 5 66
6.6 Inter-zone Connections - Example 1 70
6.7 Inter-zone Connections - Example 2 71
6.8 Inter-zone Connections - Example 3 72
6.9 Inter-zone Connections - Example 4 73
D.1 Network Dataflow 118
D.2 Network Dataflow with Zones 123
D.3 Zone A Partition 125

1 INTRODUCTION

1.1 Scope

This document is a guide to the analysis of the risk associated with the electronic processing of information which is classified as National Security Material or Sensitive Material in accordance with the Protective Security Manual (PSM) [1].

In this document, the analysis of risk is primarily concerned with the security requirement for confidentiality, the requirement whereby information is disclosed only to those users authorised to access that information.

Throughout these guidelines it is assumed that the necessary communications and compromising emanations (eg. electronic, acoustic, etc) security requirements as specified in the PSM (Part 6) are or will be satisfied.

The assessment of risk involves the consideration of the factors which contribute significantly to likelihood of unauthorised disclosure of information. This document is restricted to the consideration of those factors which directly relate to ***logical*** computer security (COMPUSEC). Physical, administrative, and procedural security factors are only considered as possible secondary influences on the strength of the COMPUSEC factors. Consideration of communications security (COMSEC) is restricted to the security functionality issues relating to network interconnections. Electronic emanations security (TEMPEST) factors are not considered in this document.

1.2 Purpose

The purpose of this document is to provide guidance to Australian Government agencies, both defence and civilian, on the specification and selection of trusted computing systems and products to be used for the electronic processing of National Security and/or Sensitive Material.

The document provides a method for the measurement of the risk of unauthorised disclosure of information in specific computer environments and the specification of the minimum level of safeguards, in the form of Trusted Computer Systems (TCSs), required to counter this risk.

2 BACKGROUND

2.1 Requirements of the Guidelines

In the process of formulating these guidelines, particular consideration has been given to the following requirements:

a. ***Applicability to Australian Government Users***
The guidelines must cover Australian Government computer systems, both in the defence and civilian sectors. It is assumed that the information processed on the system is subject to formal security classification controls and the users of the system are subject to formal security clearance controls, these controls being specified in the PSM.

b. ***Give guidance in terms of the use of TCS products to reduce COMPUSEC risks***
TCSs are designed specifically to counter COMPUSEC risks. A number of TCS products are commercially available. Consequently, the use of appropriate TCS products should be encouraged to counter COMPUSEC threats.

c. ***Applicability to Computer Networks***
It is envisaged that many of the users of the guidelines will be planning or re-configuring computer networks. Hence, guidance on the risks specifically related to computer networks must be given.

d. ***Use of Quantitative Methods***
The different classes of TCSs which have been defined have quantifiable differences in COMPUSEC functionality and assurance. In order to choose a particular class of TCS, the amount by which the risk is to be reduced to an acceptable level must also be quantified.

e. ***Establish a balance between a complex risk assessment technique and ease of application***
The guidelines should specify a risk assessment technique which can be easily understood and applied yet be sufficiently sophisticated to preclude a significant over-statement or under-statement of risk due to coarse measurement techniques.

f. ***Compatibility with Australia's Allies***
For National Security classifications and Designated Security Assessment Position (DSAP) clearances, there is a requirement to maintain compatibility with the equivalent classifications and clearances of Australia's allies.

g. ***Consistency with the US Yellow Book***
The US National Computer Security Center documents Computer Security Requirements — Guidance for Applying the DoD TCS Evaluation Criteria in Specific Environments [2] (commonly referred to as the Yellow Book), together with a Technical Rationale [3], provide a methodology for establishing which class of TCS, as defined in the US DoD Trusted Computer System Evaluation Criteria (TCSEC) [4], is required as a minimum in specific US environments. A major consideration in the production of this document is consistency with the Yellow Book standard for reasons of compatibility with Australia's allies. In order to achieve consistency, a number of assumptions have been made as to what is regarded in the Yellow Book as a "typical" system in terms of environmental characteristics.

h. ***COMPUSEC product Evaluation Criteria***
In order to determine the most suitable COMPUSEC product in a given environment, it is necessary to appraise the security features offered and the level of confidence in the operation of those features against a standard set of criteria. Since the majority of available COMPUSEC products are developed outside Australia (specifically in the US and Europe) and accredited to the security standards indigenous to the country of origin, it is necessary to provide consistent mappings of the risk index onto each of the most significant international evaluation criteria.

i. ***Focus on Confidentiality Issues***
In order to produce useful COMPUSEC risk analysis guidelines as soon as possible, one main area of risk should be the focus. The priority area here is confidentiality (i.e. cases where unauthorised disclosure would cause some damage).

j. ***Provision of a foundation for inclusion of Integrity Issues***
The next priority in areas of risk is integrity (i.e., cases where unauthorised modification or deletion would cause some damage). While COMPUSEC issues relating to integrity will not be addressed now, provision should be made in the guidelines (as far as possible) to facilitate inclusion of guidance in this area at a later date.

k. ***Consideration of non-standard Secure Connections***
A secure network architecture can include components which are not general purpose TCS products but which enhance the overall computer security. The guidelines should take into account the use of such products.

2.2 Existing Risk Analysis Approaches

In order to establish the most suitable approach to risk analysis in the context of this document, it has been necessary to conduct a thorough review of what is considered to be the most significant risk analysis approaches currently available.

For each approach reviewed, the limitations to their applicability in the Australian context are discussed.

For convenience, the approaches considered have been broadly categorised according to the type of application, either military or commercial, for which they were originally developed. However, it should be emphasised that this distinction is by no means clear-cut since many of the "commercial" approaches have been applied in military environments.

The results of this review are summarised below.

2.2.1 Military-Based Approaches

These approaches are all specifically applicable to defence environments and have the following features in common:

1. they are COMPUSEC specific;
2. they are quantitative;
3. they focus on confidentiality;
4. they use a non-financial asset measurement system based on national standard security classification levels;
5. they use a user threat measurement system based on national standard security clearance levels;
6. they have limited applicability outside the country of origin due to the fact that each country's national security classification and clearance levels may not be directly comparable;
7. the basis for measurement of risk is the degree of mis-match between the highest classification of material that the system protects and the lowest clearance level of any of the system's authorised users with adjustment due to the influence of "environmental" factors, varying in the degree of sophistication;
8. they are consistent with the Yellow Book; and
9. the minimum recommended safeguards are measured in terms of national evaluation criteria.

2.2.1.1 Yellow Book

The limitations to the applicability of the Yellow Book are assessed as follows:

1. Data sensitivity and user clearance levels reflect US national security conditions. These conditions are not always relevant in the Australian national security context. However, it is possible to map the Australian sensitivity and clearance levels to their US counterparts.
2. The treatment of categories does not hold in the Australian context where caveats or compartments are present.
3. The generic environment in which the system operates receives only limited consideration. The sole environmental distinction made is that between "open" and "closed" environments. The definition of a closed environment is of such a restrictive nature that it is unlikely to be applicable in the majority of cases.
4. The coarseness of the risk measurement technique may, in some circumstances, result in an over-statement of risk with the subsequent recommendation of a TCS which of a higher class than is actually required. This may lead to an economically infeasible solution.
5. The formula for the calculation of the risk index is inconsistent. There exists a stated anomalous case in the calculation of the risk index (i.e. TS(BI) clearance with TS data).
6. There is no rationale behind the treatment of categories and no indication of how to differentiate between hierarchical and non-hierarchical categories.
7. There is a heavy reliance on qualifying footnotes in the various rating tables in order to handle special cases.
8. There are references to other factors which may influence the final TCS class (e.g. high volume of information at the maximum data sensitivity, large numbers of users with minimum clearance, integrity and denial of service requirements) but there is no indication as to how these factors should be treated.

2.2.1.2 Landwehr and Lubbes

The paper "Determining Security Requirements for Complex Systems with the Orange Book" [5] co-authored by Landwehr and Lubbes provides, in some respects, a more comprehensive guide to the application of the Orange Book (TCSEC) in specific environments. Additional factors which affect the actual system risk are introduced with different levels of risk for each factor. The factors introduced are as follows:

Local Processing Capability;
Communication Path; and
User Capability.

An overall system risk rating is derived from the aggregation of these factors. This system risk rating and the data exposure risk index (calculated as per the Yellow Book) are combined to produce a mapping onto the TCSEC classes. The limitations to the applicability of this methodology are assessed as follows:

1. The System Risk factors are not genuinely orthogonal since all these factors relate to the scope of the user interface.
2. The issue of open and closed security environments (as defined in the Yellow Book) is not considered in this methodology. For simplicity's sake, all environments are considered to be open.
3. The majority of the levels within these factors relate to outdated features (e.g. store/forward) which are unlikely to be applicable in the context of current systems.
4. In certain cases, more than one TCSEC class is recommended for a Data Exposure / System Risk combination but no guidance is given on which to select.
5. The majority of deviations from the Yellow Book selections occur where all users have access to the computer via "dumb" terminals which is unlikely to be the case in modern practice.
6. Networks have not been considered.

2.2.1.3 DADPSWG/88-1

The UK Defence ADP Security Working Group produced a guide to COMPUSEC requirements in specific environments [6]. This guide recommends a TCSEC class based on a risk index, calculated using a similar method to that used in the Yellow Book, and a system qualifier, determined according to the characteristics of the system. The guide attempts to separate security requirements into functionality and assurance so as to allow more appropriate combinations than those specified in the TCSEC.

Unlike the Yellow Book and Landwehr and Lubbes, ancillary factors related to data sensitivity and user clearance are considered when calculating the risk index. These factors are as follows:

Total number of users;
Volume of Data;
Mix of Data; and
Special Data Separation Requirements.

The system qualifier is determined by the level of the ***Software Production Standards***, extending the Yellow Book concept of security environments, and the ***Scope of the User Interface***, an interpretation of the Landwehr and Lubbes system factors.

The limitations to the applicability of this methodology are assessed as follows:

1. Data sensitivity and user clearance levels reflect UK national security conditions. These conditions are not always relevant in the Australian national security context. However, it is possible to map the Australian sensitivity and clearance levels to their UK counterparts. This possible mapping does not extend to the treatment of caveats/compartments.
2. For the data characteristic factors ***Volume of Data*** and ***Mix of Data*** the boundary values are stated as "arbitrary to a degree" with no justification given for the values.
3. For the system characteristic ***Scope of the User Interface*** the measurement of strength is purely in terms of the terminal type and does not take into account the level of system commands available to the user.
4. No account is taken of the potential threat to the system from the external environment.
5. It is unclear how the functionality level and assurance level may be used in combination to determine the most cost effective TCS product.
6. The methodology focuses on the consideration of TCSEC criteria.
7. The methodology does not provide clear guidance on how to deal with networks.

2.2.1.4 Logicon

This approach, outlined in "A Guide to Effective Risk Management: Decision Support System" [7], uses the basic notion of data exposure, as defined in the Yellow Book, to arrive at a preliminary TCSEC class. A number of risk factors (including those identified by Landwehr and Lubbes) are considered, each with a range of weighting values corresponding to different generic environmental types. The weighting values are summed and suggested "feasible actions" are given regarding adjustments to the preliminary TCSEC class, ranging from a decrease by two levels to an increase by one level dependent on the value of the sum.

The limitations to the applicability of this methodology are assessed as follows:

1. The analysis approach is complex and is intended to be automated in the Effective Risk Management (ERM) Decision Support System, although the procedure can be done manually. With a total of 15 classes of risk factors to be considered, each having a range of possible divisions (e.g. low, medium, high), the risk of the system perpetuating erroneous subjective judgements is high.
2. Many of the risk factors are related, which is stated as a deciding factor in the assignment of weightings.
   " *However, for simplicity, the many complex interdependencies among them were disregarded and the risk factors were treated as mathematically independent entities.* " [7]. Clearly, such factors as ***User Capability*** and ***I/O Device*** are inexplicably connected.
3. The factor ***Mission Criticality*** is connected with availability rather than confidentiality.
4. The three communication-related factors are not significant since the user I/O bandwidth "bottle-neck" is more likely to be the terminal interface rather than the communication line speed.
5. The TCSEC level adjustment table has a number of footnote qualifications.
6. Network considerations are restricted to the single trusted system view. Here, the guide states that the risk factor ***I/O Device*** should be ignored. The rationale for this is not clear.

2.2.1.5 ANSSR

This approach is described in the paper "ANSSR: A Tool for Risk Analysis of Networked Systems" [8]. ANSSR performs three levels of analysis,

i. a simple Yellow Book heuristic, where a TCS class is recommended based on the standard Yellow Book inputs;
ii. a more complex risk index heuristic, based on Landwehr-Lubbes and Logicon work, extended to address risk factors associated with networking, including the cascading problem; and
iii. a scenario-based analysis, which shows ways deliberate attacks on a network could proceed and be countered by system security features. The analysis is a continuously variable measure of risk based on threat scenarios which are a succession of pre-identified events leading to an event with disclosure impact. The analysis allows either of two definitions of risk: single occurrence of loss (SOL) and annualised loss expectancy (ALE).

The limitations to the applicability of this methodology are assessed as follows:

1. The scenario analysis is complex and relies on the use of specialised risk analysis software.
2. There is uncertainty about the correctness and accuracy of the algorithms for individual events.
3. The scenario analysis expresses a network risk value but does not recommend a TCS class.

2.2.2 Commercial-Based Approaches

These approaches are most commonly applied in commercial/financial environments but are intended to be sufficiently general to apply in any type of environment. These approaches have the following features in common:

1. they do not provide a generalised risk assessment approach but tend to require many specific input parameters and produce many specific countermeasures;
2. they are not COMPUSEC specific;

3. guidance on general security measures is given rather than which class of TCS product is required;
4. they do not identify the COMPUSEC functionality or the level of assurance in that functionality which is necessary to reduce the risks to an acceptable level;
5. they tend to identify specific threat/security functionality countermeasure pairs many of which are of a non-COMPUSEC nature;
6. they tend to be more subjective than the military-based approaches and their generally complex nature tends to compound this subjectivity producing exaggerated results;
7. they are partially or wholly implemented as automated packages; and
8. the cost/benefit assessment is based on the identification and valuation of assets in monetary terms.

2.2.2.1 Asset-driven Approaches

These approaches are based on the formulation of an inventory or "checklist" of assets together with the possible threats against those assets and the vulnerabilities of the system to those threats.

An ALE is calculated, in monetary terms, for each threat event based on the estimated cost of impact on an asset from the event given the likely frequency of occurrence of the event and the probability of the event successfully impacting the asset.

The safeguards required to counter the threats are identified and a cost/benefit plan is formulated to reduce the risk.

Advantages of these approaches are:

1. the techniques used are simple and can be applied in any situation; and
2. they produce detailed asset inventories.

Disadvantages of these approaches are:

1. a significant amount of data collection effort is required;
2. there is an inability to substantiate logically the safeguard effectiveness estimates; and
3. the nature of the estimates is arbitrary.

Examples of this type of approach are the US National Bureau of Standards (NBS) Guideline for Automatic Data Processing Risk Analysis [9] and the Courtney method [10].

2.2.2.2 Function-driven Approaches

These approaches are characterised by "matrix" methods based on threats verses organisational functions (rather than specific assets). The approach is based on the concept of business dependence rather than computer vulnerability and models the functions the system supports rather than the methods employed to carry out these functions.

Critical functions are identified together with the threats which apply to those functions, the vulnerabilities corresponding to each threat and the safeguards which apply to each vulnerability. A minimum set of safeguards is selected based on the number of times a particular safeguard is deemed to be required for each type of vulnerability.

Advantages of these approaches are:

1. the functions to be examined can be specified by the user.

Disadvantages of these approaches are:

1. the choice of functions to be examined is open to subjective considerations; and
2. the volume of entries required to complete a matrix describing a system leads to imprecise measurement of impact levels.

An example of this type of approach is described in the paper "A Matrix/Bayesian Approach to Risk Management of Information Systems" [11].

2.2.2.3 Vulnerability-driven Approaches

These approaches are based on fault logic/event tree modelling. The effect of every possible threat event on an asset is simulated by vulnerability paths organised in a logical tree structure with the loss condition (the result of a threat event) at the root. Individual events in the tree are linked to one another by either direct or logical connectors. Connectors can be assigned attributes or can have calculated attributes based on the attributes of subsidiary events.

Advantages of these approaches are:

1. the results of the application of a safeguard can be seen explicitly in terms of the inhibitions in the vulnerability paths; and
2. the generation of scenarios is facilitated by these approaches.

Disadvantages of these approaches are:

1. the complexity of the models; and
2. the subjective nature of asset identification and evaluation leads to unreliable estimates of impact costs (this equally applies to the other approaches).

An example of this type of approach is the CCTA Risk Analysis and Management Methodology (CRAMM) [12].

2.2.2.4 Qualitative Approaches

These approaches are based on automated "expert" systems whereby a user inputs qualitative "guesses" and the system outputs a quantitative computed result. Rather than expressing attributes in terms of absolute values such as percentages or dollars, users may express their opinion in levels, such as low, medium and high, qualified by a confidence level.

Using the technique of fuzzy estimating, the system computes a value, with a probability that the value is what was meant, based on the context of the problem and the expert knowledge built into the system.

Advantages of these approaches are:

1. they can be used dynamically to perform risk assessments using a number of different scenarios.

Disadvantages of these approaches are:

1. they rely on complex software packages.

An example of this type of approach is the Los Alamos Vulnerability/Risk Assessment (LAVA) System [13].

2.3 Adopted Approach

The adopted approach is one which is related to the military-based approaches described above, rather than the commercial-based approaches. The approach taken was essentially an outcome of the requirements of the guidelines, with due consideration given to the assessed limitations of the existing approaches. It represents a balance between the need to provide an accurate, objective method for the measurement of risk and the need to produce a concise, usable guide.

The guidelines are primarily concerned with the confidentiality security requirement. Issues relating to the integrity security requirement which have a bearing on confidentiality are noted.

The Australian security classification and clearance controls, as described in the PSM, form the basis for the risk measurement. In order to fulfil the requirement for compatibility with Australia's allies, the guidelines provide a set of equivalence tables for Australian/US and Australian/UK classification and clearance levels.

The method adopts the basic Yellow Book factors, Minimum User Clearance and Maximum Data Sensitivity, as a foundation for the calculation of a risk index. Additionally, significant ancillary factors

relating to specific attributes of the system (associated with either data, user, or system) have been introduced. The factor strength measurement scale is roughly equivalent to that used in the Yellow Book based on the Australian/US national security classification/clearance level equivalences. The choice of these factors was influenced by the Landwehr and Lubbes system factors, the Logicon vulnerability factors, and the DADPSWG/88-1 ancillary factors. For each factor, a set of values are specified representing the levels of strength of the factor (this may range from present/absent to several levels of strength). The level of subjectivity is restricted to the judgement by the user of the appropriate level for each of the factors given their specific environment.

The method for arriving at an overall risk index is influenced by Landwehr and Lubbes. The method involves the identification of the different groups of users of the system (e.g. system administration, analysis, development, etc). For each user group, a risk assessment is performed and a risk index is obtained. The overall risk index is taken to be the worst case of the risk indices from all the user groups. This method, whereby the risk is contained within each group of the users, may result in risk index value which is lower than that resulting from an assessment where all the users are considered as a single group.

The risk assessment mechanism is table driven, producing an integer value. In common with the Yellow Book, a Data Exposure Risk Index (DERI) is calculated as a function of the Minimum User Clearance (of the user group), the Maximum Data Sensitivity, and the Exposure of Categories which, unlike the Yellow Book, is treated as a separate factor. In the case where the data-related and user-related ancillary factors are to be considered, the DERI is adjusted to take these into account. The risk index is a function of the DERI value and any system-related ancillary factor weightings. The user of the guidelines may wish to ignore the ancillary factors and perform the equivalent of a Yellow Book assessment. In this case the results will be consistent with the Yellow Book given the same environment.

The overall system risk index is mapped to a TCS evaluation level which indicates the minimum level of assurance required of a TCS given the level of risk in the environment under assessment. Guidance is also given on the TCS security functionality level required.

In the case of networks, the guidelines give advice on the choice of TCS products with respect to cost, usability and availability of products and allow alternative network architecture solutions to be analysed in terms of the fulfillment of the security requirements. The network may be decomposed into separately assessable components. In order to ensure that the network as a whole satisfies the security requirements, the rules for the secure interconnection between the network components are specified. The guidelines provide a description of the special purpose interconnection devices which enable non-standard secure connections to be established between the components of a network. These devices are themselves treated as separate network components and a separate risk assessment should be carried out on each to establish a minimum level of security criteria.

2.4 COMPUSEC Evaluation Criteria

Both the recommended minimum level of COMPUSEC functionality, as well as the recommended minimum level of assurance that the COMPUSEC functions perform correctly are expressed in these guidelines in terms of the criteria specified by the Information Technology Security Evaluation Criteria (ITSEC) [14]. The ITSEC form the harmonised criteria of France, Germany, the Netherlands, and the UK.

The ITSEC defines criteria for assessing trusted systems and products (termed Targets of Evaluation) according to the level of security functionality and the level of correctness of implementation of that functionality. Unlike TCSEC, there is no required link between the functionality specified and the level of assurance claimed. There are ten predefined functionality classes, the first five (F-C1, F-C2, F-B1, F-B2, and F-B3) corresponding to the functionality offered by the TCSEC classes C1 to B3 inclusive. The remaining five classes (F-IN, F-AV, F-DI, F-DC, and F-DX) are intended to match common requirements for particular types of system. There are seven evaluation levels, E0 to E6, which signify the level of assurance in the correctness of the corresponding security functions.

For users wishing to consider TCS products which have been evaluated against other criteria, mappings of the ITSEC criteria onto the TCSEC criteria and the UK Government Communications Headquarters (GCHQ) Communications Electronics Security Group (CESG) criteria [15] are provided in Appendix C.

It is envisaged that the majority of products which are likely to be considered will have been accredited against at least one of these criteria.

2.5 A Comparison with other military-based approaches

Table 2.1 provides a summary of the major features offered by the military-based risk assessment approaches which have been reviewed.

Table 2.1 A Comparison of Features offered by the military-based Risk Approaches

A Comparison of Features offered by the military-based Risk Approaches						
	Yellow Book	*Land-wehr and Lubbes*	*DADP-SW/88-1*	*Logicon*	*ANSSR*	*These Guide-lines*
Is consistent with the Yellow Book security requirements	*	*	*	*	*	*
Uses the basic Yellow Book approach to initial DERI calculation	*	*		*	*	*
Applicable under US National Security Conditions	*	*		*	*	
Applicable under UK National Security Conditions			*			
Applicable under Australian National Security Conditions						*
Applicable under Australian Civilian Government Conditions						*
Based on TCSEC criteria	*	*	*	*	*	
Based on ITSEC criteria						*
Separates Functionality and Assurance criteria			*			*
Addresses TCS network connectivity					*	*
Gives guidance on limited functionality network interconnection devices						*
Takes into account system factors other than Open/Closed security environment		*	*	*	*	*
Takes into account the threat from the external operating environment				*		*
Takes into account ancillary data factors			*	*	*	*
Takes into account ancillary user factors			*	*	*	*
Incorporates an automated software package				*	*	
Separates users into groups for risk assessment		*				*

A summary of the various method used to establish which level of TCS is required as a minimum in order to counter the risk of data exposure is given below.

2.5.1 Yellow Book Method

The following steps are required to perform a risk assessment:

1. calculate by look-up table the Minimum User Clearance rating;
2. calculate by look-up table the Maximum Data Sensitivity rating;
3. calculate a risk index using a function; and
4. map by look-up table the risk index to the TCSEC levels (one table for each type of security environment).

2.5.2 Landwehr and Lubbes Method

The following steps are required to perform a risk assessment:

1. calculate by matrix the Process Coupling Risk as a function of the risk factors local processing and communication path;
2. calculate by matrix the System Risk as a function of the Process Coupling Risk and the risk factor user capability;
3. calculate the Data Exposure rating in the same manner as the Yellow Book Risk Index; and
4. map by matrix the System Risk and Data Exposure to the TCSEC levels.

2.5.3 Logicon Method

The following steps are required to perform a risk assessment:

1. answer questions relating to system risk factors;
2. determine preliminary TCSEC value based on the application of the Yellow Book using the answers to the data exposure questions;
3. multiply values of the remaining data exposure questions and remaining classes of risk factors by the appropriate division value;
4. sum the products of the multiplications;
5. follow the guidance as directed by value of sum to determine the validity of the preliminary TCSEC value; and
6. apply cost, network, assurance considerations and re-evaluate.

2.5.4 ANSSR Method

The following steps are required to perform a risk assessment:

1. perform a Yellow Book Assessment specifying a target TCSEC class;
2. perform an extended Yellow Book assessment, inputting a number of attributes relating to disclosure asset, user community, and other systems;
3. for networks, assess the risk in terms of the existence of cascade paths;
4. perform a Scenario Analysis by identifying specific threat events; and
5. calculate the risk in terms of SOL and ALE.

2.5.5 DADPSWG/88–1 Method

The following steps are required to perform a risk assessment:

1. Assess the TCSEC functionality level requirements using a 3–dimensional matrix, based on Highest Classification of Information, Lowest User Clearance, and Mode of Operation.
2. Assess the TCSEC assurance level requirements. This is done as follows:
   a. calculate by matrix the user clearance rating as a function of the Lowest User Clearance and the Number of User;
   b. calculate by look-up table the overall data qualifier as a function of Volume of Data, Mix of Data, and Special Data Separation Requirements;

c. calculate by matrix the data sensitivity rating as a function of the Highest Classification of Information and the overall data qualifier;

d. calculate the risk index as a function of the user clearance rating and the data sensitivity rating;

e. calculate by look-up table the system qualifier as a function of the Software Production Standards and Scope of User Interface; and

f. map by matrix the system qualifier and risk index to the TCSEC levels.

Of the methods specified here, these guidelines most closely follow the DADPSWG/88-1 method. However, there are a number of significant differences between the two. Table 2.2 summaries these differences.

Table 2.2 Comparison of Risk Assessment Methods between these Guidelines and DADPSWG/88-1

Comparison of Risk Assessment Methods	
DADPSWG/88-1	***These Guidelines***
Applicable to UK conditions	Applicable to Australian conditions
Restricted to defence systems	Applicable to defence and civilian government systems
Requirements focus on the TCSEC criteria	Requirements focus on the ITSEC criteria
No test for cascade paths	Heuristic algorithm for network interconnection
No description of network connection devices	Description of network connection devices
No rationale for the development of the risk model	Rationale for the development of the risk model
Limited rationale for the risk index calculations	Comprehensive rationale for the risk index calculations
Limited rationale for the risk factor rating values	Comprehensive rationale for the risk factor rating values
User and data ancillary factor weightings do not take into account the level of user clearance or data sensitivity	User and data ancillary factor weightings take into account the level of user clearance or data sensitivity
User ancillary factors restricted to Number of Users	User ancillary factors include Number of Users and Proportion at Lowest Clearance
External environment not considered as a system factor	External environment included as a system factor
User Interface is represented by a single factor	User Interface is represented by three factors
User and data ancillary factor weightings applied at source	User and data ancillary factor weightings applied after the DERI is calculated
Risk assessment performed on whole user population	Risk assessment performed on user subgroups

3 RISK MODEL

To perform an assessment of risk in a particular system environment it is necessary to be able to describe that environment in terms of a discrete set of characteristics or factors which have an influence over risk.

In order to achieve this objective, a risk model has been developed. The model is a representation of the attributes of the system, in terms of the data residing on the system, the users of the system, and the system environment, which together determine the level of risk relating to the unauthorised disclosure of information. This model applies specifically to Australian government computer systems.

The model has been developed by considering the major components of risk. For each of these components, the entities which specifically relate to the model are identified and the attributes of these entities are considered.

Each significant attribute is represented in the model by a risk factor.

3.1 Assets

The assets of a computer system may be categorised as follows:

- hardware;
- software;
- information; and
- personnel.

The following assets, which will be referred to as ***Data*** hereafter, are included in the model.

1. ***Software***
   All non-TCB software is to be included. Its sensitivity level should be sufficient to permit authorised users of it to have read access. Typically, this will be the level at which the lowest cleared authorised user can gain read access.
2. ***Information***
   All information stored and processed on the system is to be included. This includes documentation (except hardcopy documentation which is not included in the model since it is protected by physical safeguards), system administration / control files, and all other types of information.

The following assets are ***not*** included in the model.

1. The TCB software is not included since it is a countermeasure and not an asset in the sense defined here.
2. The security audit file is not included since it is essential that the file be processed at system high. The high sensitivity level of the file may not be representative of the sensitivity of the majority of its records and therefore could result in a spurious assessment of the risks relating to data volume and data distribution. This equally applies to all other operating system log files.
3. The hardware and personnel assets are not included since they are protected by non-COMPUSEC safeguards.

This aspect of the model is represented in Figure 3.1.

3.1.1 Data

The data assets in this model are in the form of classified material which may be of two types — National Security and Sensitive. Both types of material may co-exist on the same computer system.

3.1.1.1 National Security Material

This material includes data (in any form and on any storage medium) dealing with or associated with the protection of Australia's or, through international agreements, another country's security, defence, international relations, and national interests.

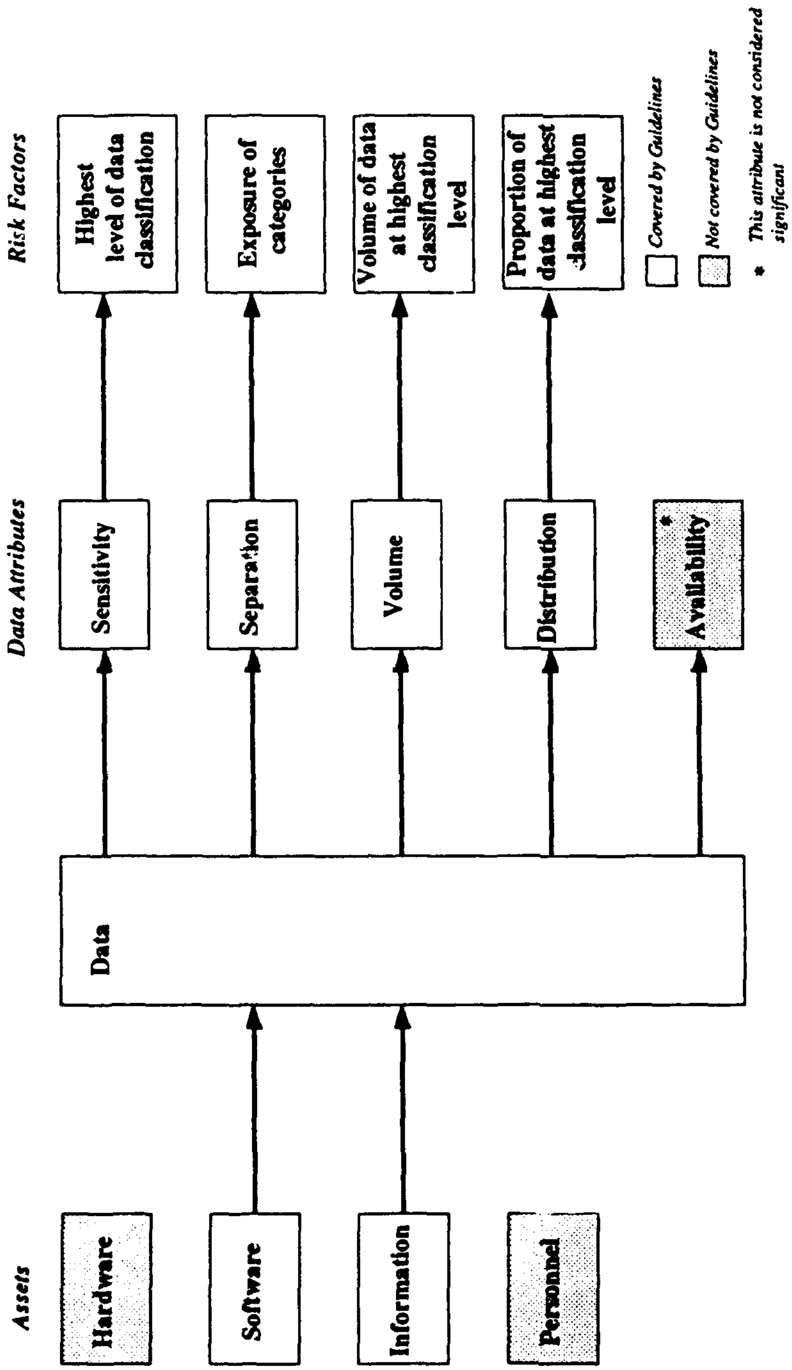


Figure 3.1 Risk Model — Assets

3.1.1.2 Sensitive Material

This material includes data, other than National Security Material, which requires protection to prevent:

a. harm (including financial harm) to the country, Government, or the legitimate activity of a Government Agency;
b. prejudice to the establishment and maintenance of lawful methods for the protection of public safety;
c. a breach of a statutory requirement to protect that material; and
d. an unfair advantage being given to any entity.

3.1.2 Data Attributes

The attributes of the data assets which may influence the risk of exposure are discussed below.

3.1.2.1 Data Sensitivity

The data assets are classified into a number of sensitivity levels based on the expected level of threat impact which is likely to be caused by the unauthorised disclosure of the data (see Section 3.4 for a description of the threat impacts).

1. ***National Security Material***
   There are four levels of National Security Material:

   Restricted (R);
   Confidential (C);
   Secret (S); and
   Top Secret (TS).

   A further pseudo-level Unclassified (U) covers material which is not classified and is considered to have no sensitivity. There is a hierarchical relationship between each of the sensitivity levels such that Unclassified < Restricted < Confidential < Secret < Top Secret.
2. ***Sensitive Material***
   There are three levels of Sensitive Material:

   In-Confidence (IC);
   Protected (P); and
   Highly Protected (HP).

   Again, a further pseudo-level Unclassified (U) covers material which is not classified and is considered to have no sensitivity. There is a hierarchical relationship between each of the classification levels in terms of sensitivity such that Unclassified < In-Confidence < Protected < Highly Protected.

In general, the relationships between the sensitivity levels of the two types of material can be described in terms of the physical protection that they must be afforded as specified in the PSM (Part 4). In this sense, Table 3.1 indicates their equivalences with respect to the recommended strength of protection mechanisms appropriate for data at each level.

Table 3.1 Relationship between the Protection level of National Security and Sensitive Material

Relationship between National Security and Sensitive Material	
National Security Material	*Level of Sensitive Material given the same level of protection*
Restricted (R)	In-Confidence (IC)
Confidential (C)	Protected (P)
Secret (S)	Highly Protected (HP)
Top Secret (TS)	†

Note
(†) There is no equivalent level.

The most conservative representation of the level of vulnerability of the data assets of a system is based on the most sensitive material which resides on the system. The strength of this attribute may be influenced by the other data attributes specified below.

This attribute is represented in the model by the factor **Highest level of data classification.**

3.1.2.2 Data Separation

There may exist at each sensitivity level one or more mandatory requirements, over-and-above the normal clearance restrictions, applicable to specific groupings of information. Access to these groupings is conditional on a security caveat which specifies special handling and need-to-know provisions. The term "caveat" is used here in the generic sense, however, for the purposes of these guidelines a more specific definition is given below.

These groups of data are termed categories. There are two types of categories.

1. ***Caveat***
   Caveated material may be accessed by a specified group of users and/or under specified circumstances for which no special briefing is required. Caveats may be characterised into the following types:

   awareness — the labelling of data with caveats warning the recipients of the sources of the information (e.g. WNINTEL);
   extensive — the extension of releasability to a set of users (e.g. releasability indicators); or
   restrictive — the restricting of distribution to a set of users (e.g. AUSTEO).

   For the purposes of assessing the risk of data exposure only restrictive caveats should be considered. Caveats cover all categories which do not fall under the definition of Sensitive Compartmented Information (SCI) and in some agencies are termed General Service (GENSER) categories.
2. ***Compartment***
   Compartmented material may be accessed only by users who have received a special briefing covering the handling of this material. Compartments are always restrictive. Compartments cover all SCI material. The sensitivity of data contained in compartments is significantly higher than data contained in caveats.

It is believed that the number of caveats or compartments present on a system does not have a significant bearing on the risk of data exposure [16]. That is, there is no significant difference between the risk associated with the exposure of a single category and the exposure of a number of categories of the same type.

This attribute is represented in the model by the factor **Exposure of categories.** This factor is only significant for systems where some users are not authorised access to all categories.

3.1.2.3 Data Volume

A first principles approach to the measure of the overall sensitivity of the data assets of a system might suggest that it would be accurately expressed as the sum of the sensitivities of data at each classification level existing on that system. The sensitivity of the data at a particular level might be measured as the product of the number of units of data at that level and a sensitivity factor for that level. The sensitivity factor is related to the amount of damage which is expected to result from the disclosure of a unit of data of a particular classification. Consequently, any measure of data sensitivity which disregards the volume of data might be expected to produce skewed results in the extreme cases. Furthermore:

1. the attractiveness of data to threat agents is related to the volume of data present on the system;
2. the likelihood of a random disclosure succeeding, given limited opportunities available to a threat agent, also is related to the volume of data present on the system; and
3. in general, the aggregate level sensitivity of information may be regarded as higher than that of the constituent parts. Although the aggregate sensitivity level is determined by the contents of the information, the volume of information is also significant insomuch as the context and the relationship between individual items of information is frequently more significant and more sensitive than are the items separately. More opportunities for heightened sensitivity through aggregation will be present with larger volumes of data.

Consequently, in certain circumstances an extremely high or low data volume warrants an adjustment to the data sensitivity rating. In order to avoid over-complex calculations, the guidelines shall confine consideration of this attribute to the highest sensitivity level, since this is the most significant level. This is in accordance with the Yellow Book which recognises the factor "*High volume of information at maximum sensitivity*" as significant.

This attribute is only significant in the situations where there are potential threat agents, i.e. systems where not all users are afforded sufficient trust to access all sensitivity levels of data on the system. These systems operate in Multilevel mode.
[Note: This attribute is not significant for systems operating in Compartmented mode since the measurement of the volume of data at the TS sensitivity level is not necessarily indicative of the volume of compartmented data. Compartmented data is taken into account by the Exposure of Categories factor].

This attribute is represented in the model by the factor **Volume of data at highest classification level,** where volume is measured as the number of bytes.

3.1.2.4 Data Distribution

Following the same argument as for the data volume, a measure of data sensitivity which disregards the spread of data over all sensitivity levels (distribution) may produce skewed results in the extreme cases. More specifically, given a random distribution of disclosures, the likelihood of a disclosure causing the greatest amount of damage possible, given the information on the system, is related to the proportion of data at the highest level of classification. Consequently, an extremely high or low proportion of data at a particular sensitivity level may warrant an adjustment to the data sensitivity rating. In order to avoid over-complex calculations, the guidelines shall confine consideration of this attribute to the highest sensitivity level since this is the most significant level.

As with data volume, this attribute is only significant in the situation where there are potential threat agents, i.e. systems where not all users are afforded sufficient trust to access all sensitivity levels of data on the system. These systems operate in Multilevel mode.
[Note: This attribute is not significant for systems operating in Compartmented mode since the compartmented data is considered to be more sensitive than TS and not distributed across sensitivity levels. Compartmented data is taken into account by the Exposure of Categories factor].

This attribute is represented in the model by the factor **Proportion of data at highest classification level.**

3.1.2.5 Data Availability

For systems which operate in different modes, the availability of data at the highest classification level may be restricted to specific periods. Hence, the opportunity for a threat agent to access this data is restricted and the vulnerability may be reduced. Since the mode of operation which is most likely to apply in these circumstances would be either Dedicated or System High where the vulnerability is regarded as low in any event, this attribute is not significant and is not represented in the model.

3.2 Threats

The threats to a computer system may be either deliberate or accidental.

Deliberate threats involve the following:

- malicious actions by humans who are authorised to have access to some or all of the data on the computer; and
- malicious actions by humans who are not authorised to access, directly or indirectly, any data on the computer.

Accidental threats involve the following:

- natural, random, and environmental events;
- malfunctioning hardware or software; and
- erroneous actions by humans who are authorised to have access to some or all of the data on the computer.

This aspect of the model is represented in Figure 3.2.

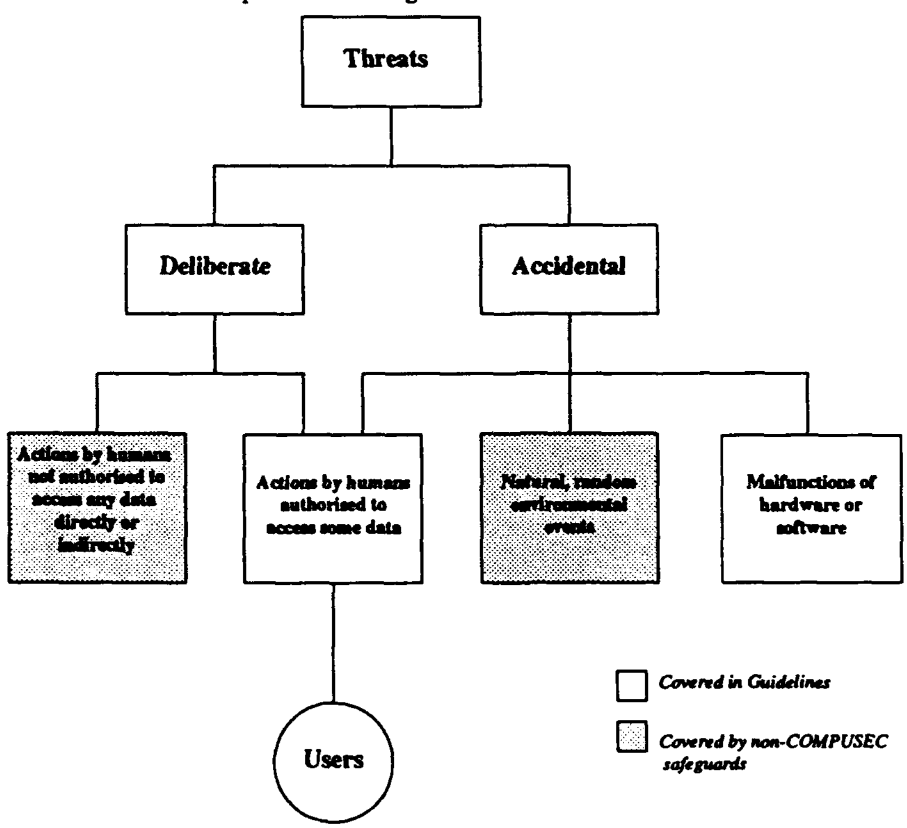


Figure 3.2 Risk Model — Threats

This model is primarily concerned with the threats posed by the deliberate or accidental action of humans who are authorised to have access to some or all of the data on the computer.

For the purposes of these guidelines, it is assumed that the safeguards required to counter the threat from humans who are not authorised to access, directly or indirectly, any data on the computer are of a non-COMPUSEC nature (i.e. physical security measures). However, if the user wishes to rely on COMPUSEC authorisation measures to counter this threat then this group must be taken into account in the risk assessment. Where this is so, it is necessary to categorise this group as potential "users" and determine their attributes. The attributes will be based on the group of humans who may gain physical access to a terminal connected to the system but have no authority to use that terminal to access the system. The existence of physical security controls on the access to terminals should be taken into account when determining these user attributes. In a situation where all persons who are authorised to have physical access to the terminal area are known, it is possible to make assumptions about the minimum level of trust based on the minimum clearance of this group. If, however, the physical security measures do not preclude the possibility of unknown users having access to the terminal area then the assumption must be that these users are potentially hostile (i.e. must be treated as uncleared users).

The likelihood of an accidental disclosure resulting from a hardware or software malfunction is a function of the level of assurance that a given Trusted Computing Base (TCB) will perform its security functions as specified by the security policy. The lower the minimum requirement for a TCS the more probable a TCB malfunction can occur. The guidelines specify that the level of assurance required of a TCS in a specific environment is that which, as a minimum, will reduce the risk associated with the probability of data exposure to an acceptable level.

The safeguards required to counter threats from natural, random, and environmental events are, generally, of a non-COMPUSEC* nature and are not considered in this model.

[Note: (*) It is reiterated here that, in the context of these guidelines, the term COMPUSEC refers to logical computer security.]

The set of humans who are authorised to have access to some or all of the data residing on the computer will be referred to as ***Users*** hereafter.

3.2.1 Users

The users of the system may be categorised as follows:

1. ***Direct Users***
   These are persons authorised to have direct access to data via a terminal connected to the system (this connection may be either local or, in the case of a network, remote but must be a component of the system); or
2. ***Indirect Users***
   These are persons authorised to have indirect access to data transferred via:

   - a terminal which is has a communication link to the system but is not considered part of the system (this may be a connection via a remote dial-up modem link or an indirect connection via another system); or
   - removable media (i.e., hardcopy, removable disk, magnetic tape, etc)

   where ***no manual review*** has been performed. Manual review is the activity, carried out by an authorised person, which ensures that the sensitivity label of the data being output from the system accurately represents the contents of the data. Data which has undergone manual review is subsequently protected by non-COMPUSEC measures and consequently persons accessing this data are not considered in this model.

The users of the system may be regarded as assets or threat agents. In this model the attributes of the users in terms of threat agents is significant in determining the risk of data exposure.

This aspect of the model is represented in Figure 3.3.

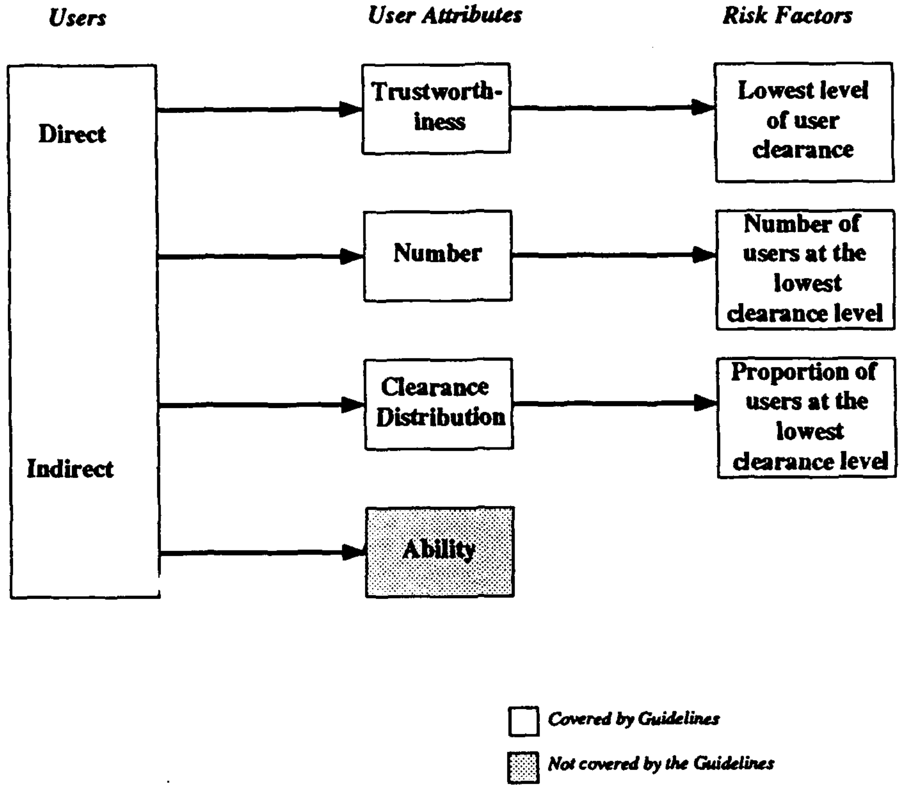


Figure 3.3 Risk Model — Users

3.2.2 User Attributes

The attributes of users, as potential threat agents, which may have an influence on the risk of data exposure are discussed below.

3.2.2.1 User trustworthiness

The level of confidence in the loyalty and reliability (trustworthiness) of a user is signified by the security clearance level granted to the user, and allows access to classified material at and below a certain classification level (in the absence of any "need-to-know" restrictions). The clearance process involves a formal security checking process. There are two types of security clearance, Designated Security Assessment Position (DSAP) and Position of Trust (PoT). Users cleared through either of these processes may co-exist on the same system.

1. ***DSAP***
   This clearance allows access to National Security Material. In order to access material which is classified above Restricted, users are required to be cleared to access at least that level of classified material. The checking process is of two types:

   Negative Vetting (NV) — used for most clearances; and

   Positive Vetting (PV) — more thorough, used for access to certain Top Secret (TS) material.

A security clearance is not required for access to Restricted (R) material, however, a need-to-know requirement must be established.

2. *PoT*

This clearance allows access to Sensitive Material or to valuable resources (e.g. money, drugs, and computer equipment). There is only one type of checking undertaken for PoT clearances. The formal clearance processes correspond to two clearance levels for access to Sensitive Classified Material:

Protected (P); and

Highly Protected (HP).

A security clearance is not required for access to In-Confidence (IC) material, however, a need-to-know requirement must be established.

No PoT clearance is equivalent to any DSAP clearance. The holder of a PoT clearance alone must not access National Security material which is classified Confidential or above. Unless otherwise specified by and for a particular organisation, a DSAP clearance can permit the holder to access Sensitive material in accordance with Table 3.2.

Table 3.2 Levels of Sensitive Material which may be accessed by DSAP cleared Personnel

Access to Sensitive Material by DSAP cleared personnel	
DSAP Clearance	***Allows access to Sensitive Material up to and including***
Confidential (C)	Protected (P)
Secret (S)	Highly Protected (HP)
Top Secret through Negative Vetting (TS (NV))	Highly Protected (HP)
Top Secret through Positive Vetting (TS (PV))	Highly Protected (HP)

Access to Sensitive material by the holder of a DSAP clearance requires that the need-to-know must be established.

The most conservative representation of the level of trust afforded any group of users of a system is taken to be the level of trust of the least cleared member of the group. The strength of this attribute may be influenced by the other user attributes specified below.

This attribute is represented in the model by the factor **Lowest level of user clearance**. This factor applies to both direct and indirect users.

[Note : For TCS classes where sensitivity labelling is a security function, the TCB is only trusted to label correctly sensitive data within a range of sensitivity levels determined by the evaluation level of the TCS. This range, which has an upper bound of the highest sensitivity level on the system, may be narrower than the full range of data sensitivity levels on the system. In this case, the TCB cannot be trusted to correctly label data at a sensitivity level lower than the lower bound of the allowable range. If data labelled at a sensitivity level below the lower bound is to be released, without manual review, to indirect users then the TCS evaluation level must be increased. In this case, the minimum TCS evaluation level is obtained by taking the Minimum User Clearance level in the DERI calculation to be that which is required by indirect users (as a minimum) to access data at the lowest label given to released data.]

3.2.2.2 Number of Users

The probability that some user of the system is a threat agent may be more accurately expressed as the sum of the probabilities, for each level of user clearance on the system, that there is a threat agent in the group of users cleared to that level. Each of these probabilities may be expressed as the product of the number of users at that level and the empirical likelihood that a user cleared to that level is a threat agent, which is related to the trustworthiness attribute. Hence, a measure of the likelihood of a threat agent which disregards the number of users at each level may produce skewed results in the extreme cases. Consequently, in certain circumstances, an extremely high or low number of users warrants an adjustment to the user clearance rating. In order to avoid over-complex calculations, the guidelines shall confine consideration of this attribute to the lowest level of user clearances since this is the most significant level. This is in accordance with the Yellow Book which recognises the factor "*Large number of users with minimum clearance*" as significant.

This attribute is only significant where there is data on the system to which the lowest cleared user is not cleared to access, i.e. systems operating in Multilevel mode.
[Note: Although this attribute may possibly be relevant to systems operating in Compartmented mode, the factor is ignored in this case since no other ancillary factors are applicable].

This attribute is represented in the model by the factor **Number of users at the lowest clearance level.**

3.2.2.3 User Clearance Distribution

Following the same argument as for the attribute Number of Users, a measure of likelihood of a threat agent which disregards the spread of users over all sensitivity levels (distribution) may produce skewed results in the extreme cases.

This attribute is only significant if there are some users who are not cleared to access all the sensitivity levels on the system, i.e. systems operating in Multilevel mode.
[Note: For systems operating in Compartmented mode, this attribute is not applicable since all users are cleared to access data at TS level].

This attribute is represented in the model by the factor **Proportion of users at the lowest clearance level.**

3.2.2.4 Ability of Users

The likelihood of a threat agent perpetrating a disclosure is influenced by the degree of expertise, system knowledge, and information available to a threat agent. While this attribute is undoubtedly significant, it is difficult to formulate a consistent discriminatory measure. Hence its influence has been removed from the guidelines by the conservative assumption that any threat agent will either possess the necessary expertise, system knowledge, and information to perpetrate a disclosure or will have access to other persons who do.

3.3 Vulnerabilities

This model considers the vulnerabilities of a computer system which have a significant effect on the frequency of occurrence and level of impact of the data exposure threat.

The vulnerabilities of a system are associated with the attributes of the assets of the system in terms of computer hardware, firmware, and software and the environment under which the system operates.
[Note: Vulnerability is also a function of the attributes of the data and the personnel (user) assets, however, these have been considered in the preceding sections.]

This aspect of the model is represented in Figure 3.4.

3.3.1 System Attributes

The attributes of the hardware, firmware and software assets and operational environment which may have an influence on the risk of data exposure are discussed below.

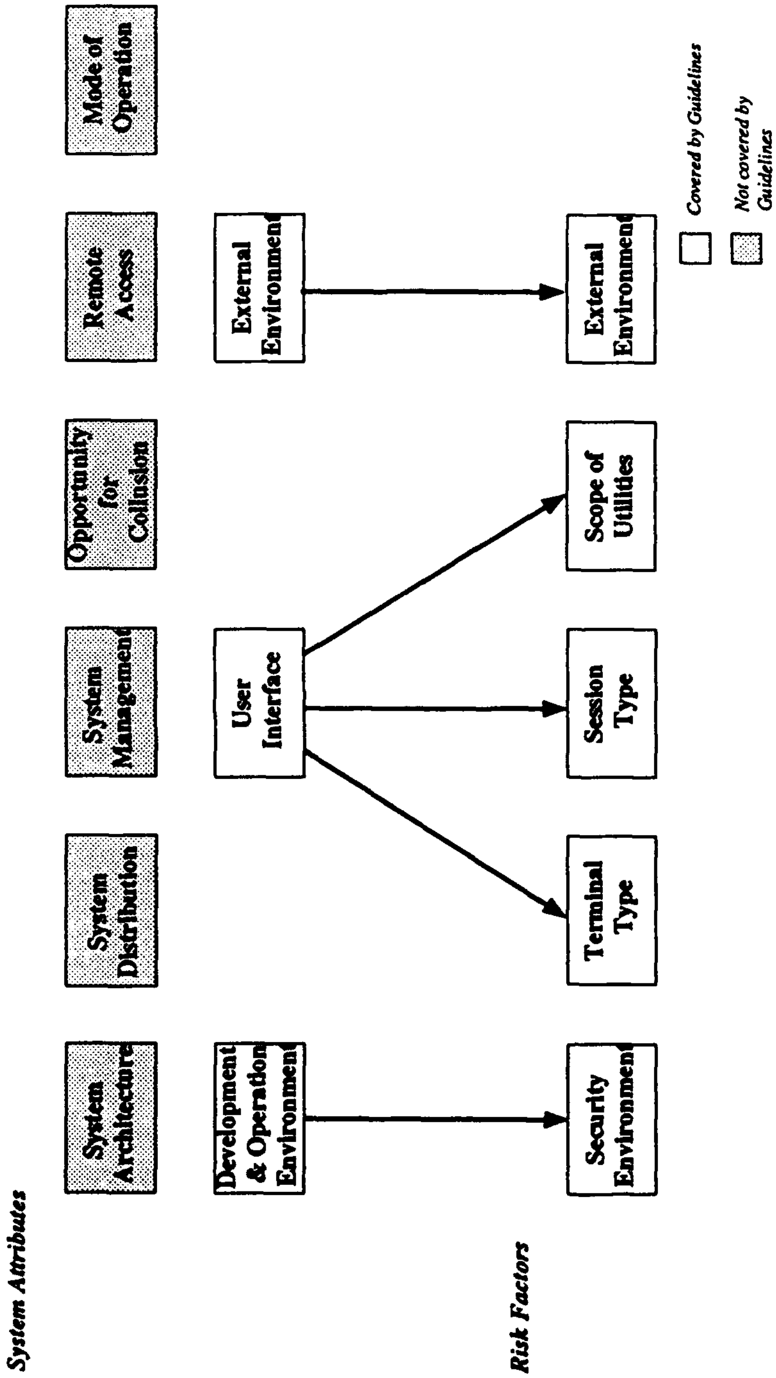


Figure 3.4 Risk Model — Vulnerabilities

3.3.1.1 System architecture

The hardware configuration (e.g. embedded, monolithic, distributed) may have an influence on the vulnerability of the system. However, within an environment which is controlled by the appropriate physical security measures, the type of system architecture is not significant in terms of vulnerability [16]. Furthermore, the specific features of a system which are likely to influence its vulnerability (e.g. intelligent terminals, remote devices, communication lines, local output facilities, etc) must be considered individually rather than attempting to generalise in terms of a generic architectural type. Consequently, this attribute is not represented in the model.

3.3.1.2 System distribution

A distributed system in a controlled environment is no more vulnerable than a centralised system in the same environment, but, the presence of unprotected communication lines which are external to the controlled environment does represent a significant increase in vulnerability [16]. However, the countermeasures required to reduce this vulnerability are of a COMSEC nature. For the purposes of these guidelines, the assumption is made that the prescribed COMSEC safeguards to counter the risk of interference with external communication lines are in place. Consequently, this attribute is not represented in the model.

3.3.1.3 System management

The degree of control over the administration of system functions (including security-related functions) may have an influence on vulnerability. This is particularly the case in a network where the system management and security management functions are distributed over a number of sites. The degree of control of the administration of the system functions has an important bearing on the risk of misuse of these functions in order to circumvent the security controls. This attribute is not represented in the model by a specific factor but is implicit in the user interface factors.

3.3.1.4 External environment

The external environmental conditions under which a system operates may have a significant influence on the number of threat agents present or, conversely, the probability of the existence of a threat agent, on a system.

The external environment may be categorised into the following levels of potential hostility.

1. ***Hostile***
   The characteristics of the external environment are such that it is highly likely that there will be at least one threat agent active on the system (e.g. a foreign embassy).
2. ***Neutral***
   The characteristics of the external environment are unlikely to influence the probability of a threat agent being active on the system.
3. ***Benign***
   The characteristics of the external environment are such that it is unlikely that there will be a threat agent active on the system (e.g. a government department central office).

This attribute is represented in the model by the factor **External Environment**.
[Note: This factor is related to the Logicon risk factor "Overall System Environment", however, the Logicon factor is more related to the degree of physical and administrative security measures in place rather than the type of location].

3.3.1.5 Remote access

In the situation where terminals, printers, or other systems outside the controlled security perimeter are connected to the system under assessment there may exist a greater degree of vulnerability due to the threat from remote users (either humans or processes) who are not known to the system. However, this attribute relates to the users of the system rather than the system itself. That is,

1. if the remote user is known to the system and appropriate non-COMPUSEC safeguards are in place then, for the purposes of the DERI calculation, the remote user should be treated in the same way as a local user; and
2. if the remote user is not known to the system or appropriate non-COMPUSEC safeguards are not in place then, for the purposes of the DERI calculation, the remote user should always be assumed to be Uncleared.

Consequently, this attribute is not represented in the model.

3.3.1.6 User Interface

Of particular significance to the vulnerability of the system is the scope and bandwidth of commands which may be input by the user, or by a process operating on the users behalf, and accepted by the system. The scope and bandwidth of commands will be influenced by the mechanisms available to the user to generate such commands (e.g. local processes and host applications).

The user interface may be described in terms of three key characteristics: terminal interface, host interface, and host services. It may be argued that a fourth characteristic, communication circuit, should also be considered since the bandwidth of commands may be influenced by the speed and the mode of the communication circuit between the terminal and the host. This characteristic does not warrant a specific risk factor for the following reasons:

1. where commands are manually generated, the bandwidth is determined by the speed of the keyboard input; and
2. where commands are electronically generated, in the case of the intelligent terminal, the bandwidth of the communication circuit is assumed to be greater or equal to the bandwidth of the command input program.

These characteristics are not truly orthogonal since the possible levels of a particular characteristic may be dependent on the levels of one or both of the other characteristics. In particular, if the user has access to an extensive set of host services then the user must be connected interactively to the host via a full-function terminal. Conversely, a user with a limited functionality keypad cannot establish an interactive session with the host.

Nevertheless, it is useful to make this distinction in order to provide a more objective measurement of the level user interface and to avoid the explicit specification of all the possible combinations.

3.3.1.6.1 Terminal Interface

The terminal is responsible for the interpretation and transmission of user keystrokes to the host and the display of data received from the host on the user's screen. The following types of terminals represent an increasing level of vulnerability to the system.

1. ***Limited function***
   These terminals have special limited functionality keypads which preclude the user from entering direct commands. Both the scope and the bandwidth of commands is severely restricted in this case.
2. ***Full function — dumb***
   These terminals have standard alphanumeric keypads which permit direct command input. The terminal may have some limited local software or firmware (e.g. read-ahead buffers) but is not capable of being programmed locally. The scope of commands is greater but the bandwidth is limited to the speed of the keystrokes.

3. ***Full function — intelligent***
   These terminals possess the capability to be programmed locally (e.g. PCs). These devices provide the user with the capability to generate commands at a high bandwidth from a process running locally in the terminal. A local process may also be capable of intercepting the output of sensitive data or the input of user identification data.
   [Note: It could be argued that a PC should be treated as separate TCS component rather than a terminal. This would require a PC-local TCB and the treatment of the system as a network where interconnection considerations apply].

This attribute is represented in the model by the factor **Terminal Type.**
[Note: This factor is related to the Landwehr and Lubbes factor "Local Processing Capability"].

3.3.1.6.2 Host Interface

The level of restrictions imposed on the allowable commands or transactions received from the terminal by the host application servicing the terminal has an influence on the vulnerability of the system. The terminal servicing program acts as a filter between the user and lower layers of system software (including the TCB). The more restrictive the filter, the less vulnerable the system is to penetration.

These modes are categorised as follows:

1. ***Output only***
   The host interface program provides predefined outputs regardless of the inputs the user presents.
2. ***Transaction processing***
   The host interface program will only accept predefined, well-formed commands. All other input is rejected by the program.
3. ***Interactive***
   The host interface program provides direct access to the operating system.
   [Note: It is recognised that in many systems there are different levels of interactive processing (e.g. application, supervisor, kernel), this is discussed under the Host Services attribute.]

This attribute is represented in the model by the factor **Session Type.**
[Note: This factor is related to the Landwehr and Lubbes factor "User Capability"].

3.3.1.6.3 Host Services

The extent to which users are authorised to utilise the operating system services (including the TCB) has an influence on the vulnerability of the system. The possibility of establishing a covert channel is greatly enhanced when the user has access to privileged commands.

This attribute is most likely to apply to interactive processing. In many systems there are hierarchical levels of processing or modes of operation (e.g. application, supervisor, kernel) with increasing access to privileged commands. Due to the relative coarseness of the risk measurement mechanism only two levels are considered:

1. ***Limited***
   System services are restricted to a basic set of non-privileged commands.
2. ***Full***
   System services are extensive and may include privileged commands which manipulate the operating system.

This attribute is represented in the model by the factor **Scope of Utilities.**

3.3.1.7 Development and operational environment

The type of environment under which application software is produced and run has an influence over the vulnerability of the system to penetration. A threat agent is more likely to succeed in exposing data when

the agent is able to utilise application software which has been specifically developed to compromise the security policy. By means of malicious logic, such application software may:

1. deliberately or accidentally perform an unauthorised modification to the TCB [Note: This is an integrity issue];
2. deliberately exploit covert or overt channels; or
3. deliberately or accidentally exploit weaknesses in the TCB.

Each of these actions may result in the unauthorised exposure of data.

The introduction of such software is less likely to occur on systems where configuration control procedures are enforced and the level of trust of the application software developers is high.

For consistency with the Yellow Book, environments are categorised as either open or closed. The definitions are taken directly from the Yellow Book.

1. ***Open Security Environment***
   "*... includes those systems in which either of the following conditions holds true:*

   a. *Application developers (including maintainers) do not have sufficient clearance (or authorisation) to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where maximum classification of data to be processed is Confidential or below, developers are cleared and authorised to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.*
   b. *Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.*

   " [3].
2. ***Closed Security Environment***
   "*... includes those systems in which both of the following conditions holds true:*

   a. *Application developers (including maintainers) have sufficient clearance and authorisations to provide an acceptable presumption that they have not introduced malicious logic.*
   b. *Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.*

   " [3].

The mechanism in the Yellow Book, whereby this factor is the sole determinant of the TCSEC level in the high risk case, has been somewhat tempered in these guidelines since the final risk index is depended on a combination of all the system factors. The lessening of emphasis takes into account the possible inadvertent introduction of malicious applications logic which may occur in both open and closed environments.
"*A recent study [17] has shown that, in many cases, there is a larger threat* [than deliberate introduction of malicious logic] *from software errors and authorized users who do not follow established procedures or who ignore system warnings. Clearly, the holder of a security clearance is no less likely to make programming errors or deviate from established procedures than someone who is not cleared.*" [7].

With the increasing trend towards the development of systems using Commercial Off-the-Shelf (COTS) application software, the applicability of a Closed Security Environment is diminishing.

This attribute is represented in the model by the factor **Security Environment**.

3.3.1.8 Opportunity for User Collusion

Where a number of threat agents are active on the same system, the likelihood of a threat event occurring is higher if these agents are acting in concert rather than in isolation. However, the security countermeasures against this type of threat are administrative rather than COMPUSEC. Consequently, this attribute is not represented in the model.

3.3.1.9 Mode of Operation

The system may be regarded as operating in one of a number of security operating modes. These modes are determined by the following factors:

1. the level of trust in the system hardware/software;
2. the range of data sensitivity levels processed;
3. the extent of user access to the data; and
4. the presence of compartments.

The number of possible modes and the definitions of these modes are subject to some inconsistences between risk methodologies. The definitions given below are taken from the Yellow Book, with the omission of "Controlled Mode" which is not significant in the context of these guidelines.

1. ***Dedicated***
   "*... the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.*" [3].
2. ***System High***
   "*... system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electronically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system, and all system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.*" [3].
3. ***Compartmented***
   "*... allows the system to process two or more types of compartmented information (information requiring a special authorisation) or any one type of compartmented information with other than compartmented information. In this mode, the system access is secured to at least Top Secret (TS) level, but all system users need not necessarily be formally authorized access to all types of compartmented information being processed and/or stored in the system.*" [3].
4. ***Multilevel***
   "*... allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present*" [3].

The mode of operation of a system is not a contributory factor to the vulnerability of the system but rather a consequence of the risk factors. The mode of operation is significant, however, when considering the following:

- the applicability of data and user ancillary factors;
- the minimum level of COMPUSEC functionality required to operate in a particular mode; and
- the minimum level of COMPUSEC assurance required to operate in a particular mode.

3.4 Threat Effects (Impacts)

The threat effects which may result from a successful attack on the data residing within a system, carried out by a user or users of that system, are as follows:

- data exposure;
- data corruption (of which destruction is a special case); and
- denial of service.

This model is primarily concerned with the impact of data exposure. Data exposure is directly related to the level of trust in the users and their agents not to utilise for malicious purposes the material accessed, regardless of whether the material was accessed deliberately or accidentally.

[Note: The argument regarding the level of trust in the users does not hold for all integrity-related effects since an impact may result directly from an accidental event, and in this case the likelihood of an occurrence is not related to the clearance level of the user. Data exposure may result from integrity-related effects such as the mis-labelling of data by a faulty TCB, and faulty or malicious untrusted software. In the case of an accidental labelling malfunction the risk of data exposure is confined to the situation whereby data is accidentally downgraded.]

The security requirements which relate to these threat effects are as follows:

- confidentiality;
- integrity; and
- availability.

The threat effects are not universally orthogonal. An integrity violation may cause a confidentiality violation. For example, the incorrect sensitivity labelling of a data item in a multilevel secure environment by TCB software may result in the exposure of that data item to users who are not authorised to access the data. [Note that as a protection against this eventuality, the Bell and La Padula Multilevel security model [18] specifies the so called *-property which restricts "write-downs"]. An integrity violation may also cause a denial of service (availability violation). For example, the unauthorised modification of system software may result in a system crash when that software is executed.

The relationship between security violations and threat effects is represented in Figure 3.5.

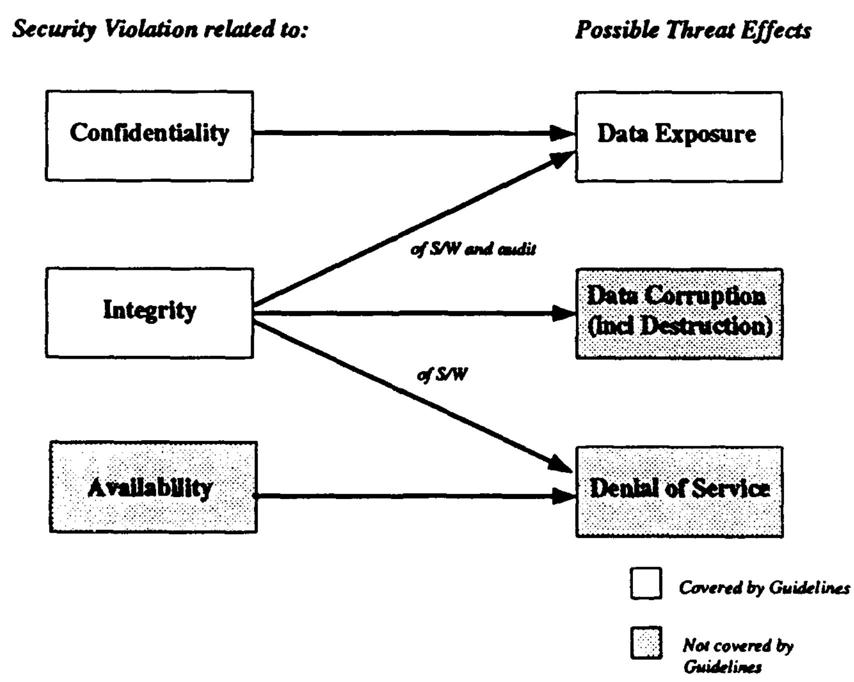


Figure 3.5 Risk Model — Threat Effects

The impact of the exposure of National Security material is measured in non-monetary terms as the level of damage to national security of Australia and/or Australia's Allies which could reasonably be expected to be result. Table 3.3 summarises the impact levels for National Security material.

Table 3.3 National Security Material — Impacts

Impacts caused by exposure of National Security Material	
Sensitivity level	***Impact***
Restricted (R)	Could possibly be harmful to national security
Confidential (C)	Could reasonably be expected to cause damage to national security
Secret (S)	Could reasonably be expected to cause serious damage to national security
Top Secret (TS)	Could reasonably be expected to cause exceptionally grave damage to national security

The impact of the exposure of Sensitive material is measured in non-monetary terms as the level of damage to any person, organisation, or Local/State/Territory government which provided information to the Commonwealth under an assurance/expectation of confidentiality or about which the Commonwealth holds information. Table 3.4.summarises the impact levels for Sensitive material.

Table 3.4 Sensitive Material — Impacts

Impacts caused by exposure of Sensitive Material		
Sensitivity level	***Impact***	
In-Confidence (IC)	Might possibly	cause harm to the country, Government or the legitimate activities of an agency
		be prejudicial to the establishment and maintenance of lawful methods for the protection of public safety
		cause harm to any person, organisation, or Local/State/Territory Government which provided information to the Commonwealth under an assurance/expectation of confidentiality or about which the Commonwealth holds information
		give unfair advantage to any entity
Protected (P)	Could reasonably be expected to	cause harm to the country, Government or the legitimate activities of an agency
		be prejudicial to the establishment and maintenance of lawful methods for the protection of public safety
		cause harm to any person, organisation, or Local/State/Territory Government which provided information to the Commonwealth under an assurance/expectation of confidentiality or about which the Commonwealth holds information
		give unfair advantage to any entity
Highly Protected (HP)	Could reasonably be expected to	cause serious harm to the country, Government or the legitimate activities of an agency
		be seriously prejudicial to the establishment and maintenance of lawful methods for the protection of public safety
		cause serious harm to any person, organisation, or Local/State/Territory Government which provided information to the Commonwealth under an assurance/expectation of confidentiality or about which the Commonwealth holds information
		give unfair advantage of significant proportions to any entity

3.4.2 Safeguards (Countermeasures)

The safeguards which may be used to counter COMPUSEC vulnerabilities may be categorised as being either:

1. standardised and available as part of existing commercial TCS product; or
2. non-standardised and developed to perform one or more specific COMPUSEC functions.

The safeguards in the former category are defined as COMPUSEC functions by COMPUSEC standards, primarily the ITSEC criteria which includes those functions identified in the TCSEC criteria. The ITSEC criteria specify the safeguards in terms of functionality classes, each class defining a minimum set of safeguards required to satisfy the functionality criteria for that class.

The safeguards in the latter category are typically employed on individual computer systems where a specific need is identified which is not fulfilled by a commercially available TCS product. These non-standard safeguards require development according to the same standards as the commercially available

products. The uniqueness of the non-standard safeguards makes detailed description of them impractical here. However, some of these products are potentially useful in a network architecture and are addressed in Section 5.

The risk analysis process described in this document is primarily concerned with the use of commercially available TCS products to counter the risk of data exposure. The use of non-standard safeguards is addressed only as part of guidance on the use of specific non-standard safeguards within a network architecture.

3.5 Risk Factor Hierarchy

The risk model represents a set of hierarchical factors which are categorised according to their representation of the attributes of the entities; data, users, and system and their relative contribution to the overall risk.

The model is represented in Figure 3.6..

3.5.1 Data Dependent Factors

These factors represent the attributes of the data assets discussed in Section 3.1.2.

3.5.1.1 Primary

These factors are considered to have a major influence on the risk of data exposure. The factors are:

> ***Highest level of data classification***; and
> ***Exposure of categories.***

3.5.1.2 Ancillary

These factors are considered to have a lesser influence on the risk of data exposure but, if combined, may have an influence on the strength of the primary factor. The significance of each of these factors is dependent on the ***Highest level of data classification***. The factors are:

> ***Proportion of data at highest classification level***; and
> ***Volume of data at highest classification level.***

3.5.2 User Dependent Factors

These factors represent the attributes of the users as potential threat agents discussed in Section 3.2.2.

3.5.2.1 Primary

This factor is considered to have a major influence on the risk of data exposure. The factor is:

> **Lowest level of user clearance.**

3.5.2.2 Ancillary

These factors are considered to have a lesser influence on the risk of data exposure but, if combined, may have an influence on the strength of the primary factor. The significance of each of these factors is dependent on the ***Lowest level of user clearance***. The factors are:

> ***Number of users at the lowest clearance level***; and
> ***Proportion of users at the lowest clearance level.***

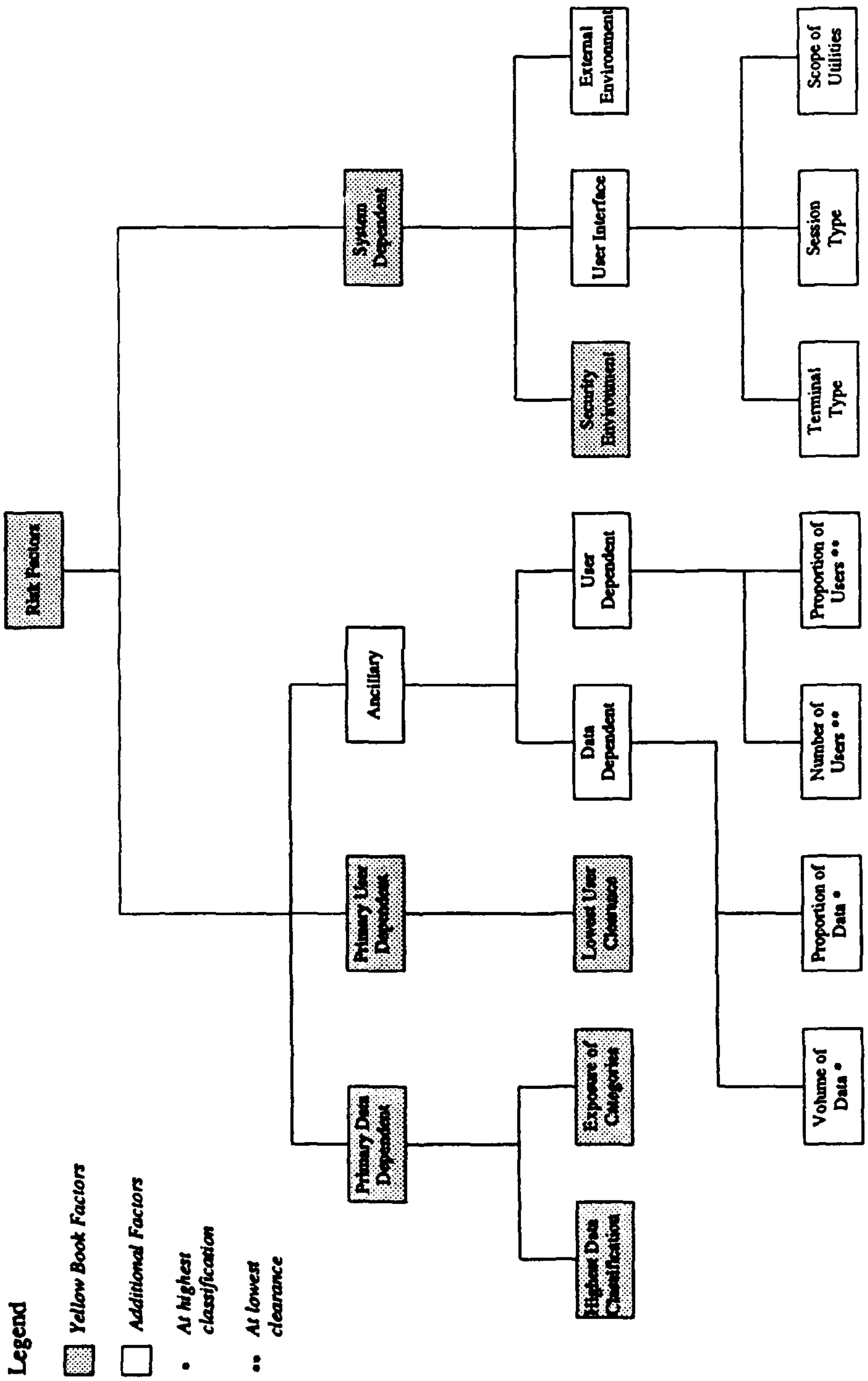


Figure 3.6 Risk Model

3.5.3 System Dependent Factors

These factors represent the attributes of the system which are significant in determining it's vulnerability to data exposure as discussed in Section 3.3.1. The factors are categorised as follows.

3.5.3.1 Environment

The factors relating to the system environment are:

> ***Security environment***; and
> ***External environment.***

3.5.3.2 User Interface

The factors relating to the user interface are:

> ***Terminal type***;
> ***Session type***; and
> ***Scope of utilities.***

4 RISK ASSESSMENT

4.1 Overview

The output from the risk assessment process is an integer value, the Risk Index, which represents a measure of the risk of unauthorised disclosure of data, given the computer system environment under assessment.

Prior to the risk assessment, it is necessary to separate the user population into functional groupings.

A separate risk assessment should be performed for each of the user groups identified, with some user-related and/or system-related factors varying between groups. The overall Risk Index value is the highest of all the group risk indices.

Each risk assessment involves the definition of the system, with respect to the user group, in terms of the security parameters; the identification of the appropriate level of each of the risk factors identified in Section 3 based on these parameters; and the calculation of a risk index value based on the factor weighting values.

It should be noted that the factor weighting values specified below represent best estimates based on current knowledge of risk assessment techniques and are not based on rigorous mathematical analysis. A certain level of crudeness and arbitrariness must be expected here due to the imprecise nature of risk quantification and the narrowness of the risk index range reflecting the limited number of TCS evaluation levels.

It is the intention of these guidelines to minimise this crudeness and arbitrariness and to avoid any compounding of inaccuracies resulting in an unrealistic risk index for particular circumstances.

Figure 4.1 provides a diagrammatic representation of the risk assessment process.

4.2 Identify the User Groups

The process of categorising users into functional groups is very much dependent on the particular system under assessment. These guidelines do not attempt to specify an exhaustive list of possible user groupings, however, the following general rule must be adhered to in order to avoid producing spurious results due to artificial groupings.

No two user groups should have ***all*** of the following risk factors in common:

> ***Lowest level of clearance***;

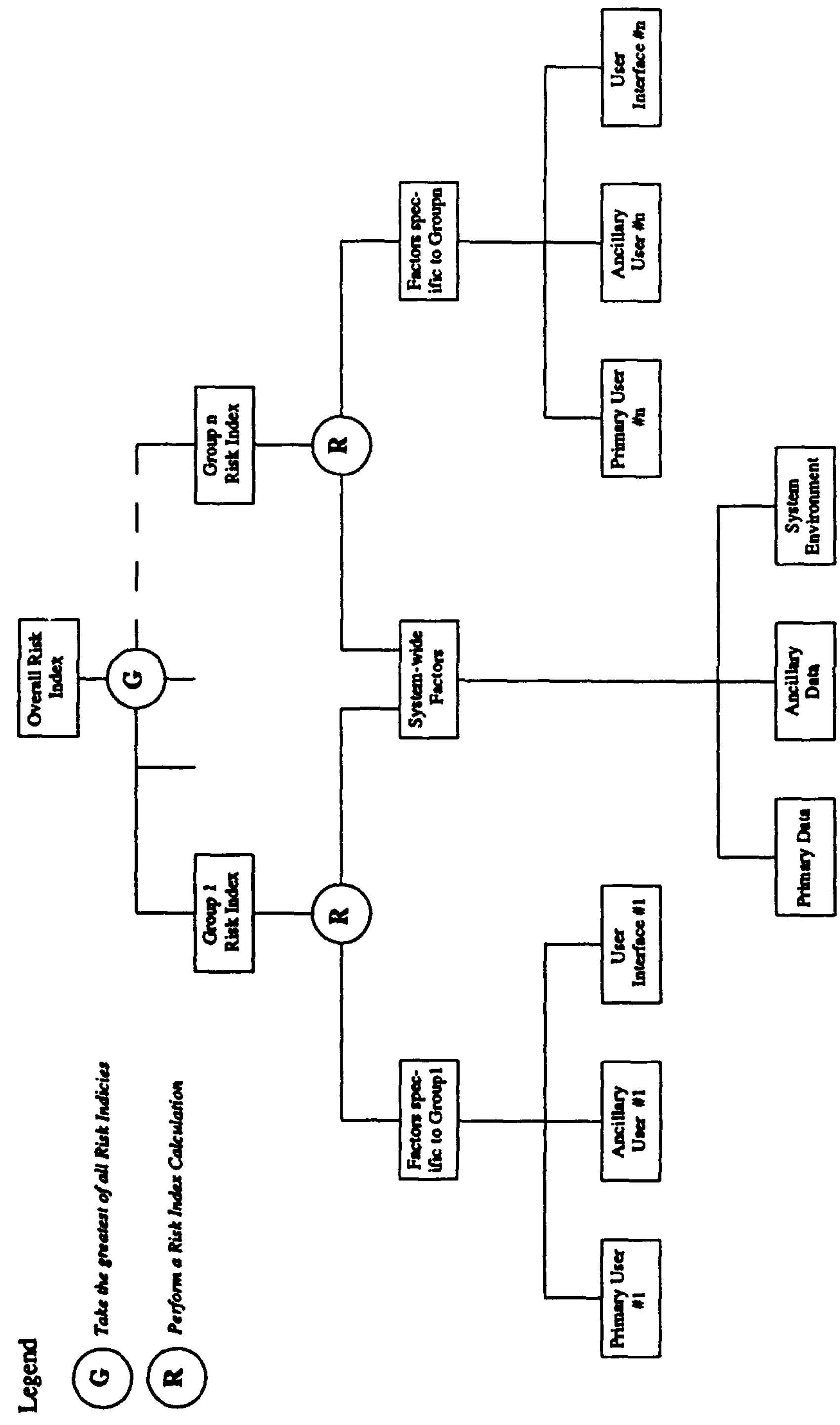


Figure 4.1 Risk Assessment Process

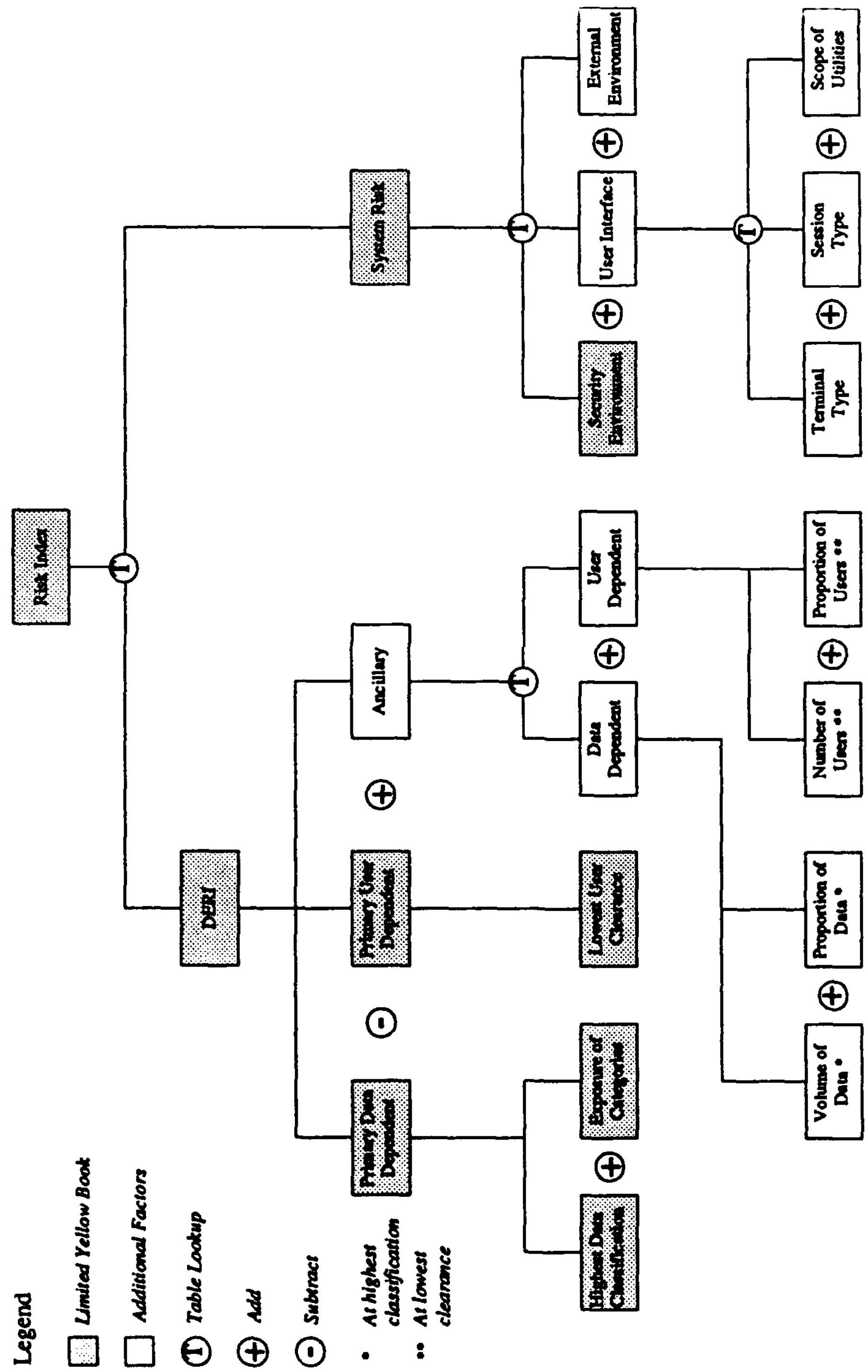


Figure 4.2 Risk Index Calculation

Terminal type;
Session type; and
Scope of Utilities.

A risk assessment specifying only one user group comprising the whole user population is not precluded.

For each user group identified a risk assessment is performed as specified in Section 4.3.

4.3 Perform the Risk Assessment

The risk assessment involves the calculation of a risk index. This calculation may be considered as a hierarchical operation which is represented in Figure 4.1. If a limited Yellow Book type assessment is required then it is possible to restrict the calculation to a subset of the hierarchy, as indicated in Figure 4.2. More generally, if any aspect of the system is considered not to be applicable, then the particular branch of the hierarchy tree relating to this aspect may be removed with no effect on the risk index calculation.

The process involves the measurement of the risk factors in the environment under assessment. It should be noted that, although the user interface factors and some system-related factors will be specific to the user group under assessment, the data-related factors and the other system factors will be the same for each user group.

In order to facilitate the assessment proforma copies of Security Parameter Record and a Risk Assessment Record are provided in Appendix A (Tables A.1 and A.2).

The following information should be recorded on the Security Parameter Record:

1. the system identity;
2. the user group identity;
3. the maximum sensitivity level of the data which resides on the system;
4. the presence of at least one category of data for which some users of the group are not authorised access;
5. the type of the most sensitive category or categories present;
6. the number of bytes of data at the maximum sensitivity level on the system;
7. the total number of bytes of data residing on the system;
8. the minimum clearance level of the users of the group;
9. the number of users of the group who are cleared to the minimum clearance level;
10. the total number of users in the group;
11. the type of user interface available to users of the group in terms of terminal type, session type, and scope of utilities;
12. the conditions under which non-TCS software is developed and run on the system; and
13. the nature of the environment under which the system operates.

With reference to the Rating Tables specified below and the completed Security Parameter Record, the Risk Assessment Record should be completed.

4.3.1 Rating Tables

4.3.1.1 Primary Data dependent Factors

Below are the rating tables for the primary data dependent factors.

Table 4.1 Rating Scale for Maximum Data Sensitivity — National Security Material

Highest level of data classification	
Unclassified (U)	0
Restricted (R)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)	5

Notes

1. The presence of categories within classification levels is to be treated as a separate factor (see Table 4.3).
2. Table B.1 gives an equivalence table for US and UK National Security data classification levels.

Table 4.2 Rating Scale for Maximum Data Sensitivity — Sensitive Material

Highest level of data classification	
Unclassified (U)	0
In-Confidence (IC)	1
Protected (P)	2
Highly Protected (HP)	3

Notes

1. The rating values reflect the relationship between the level of protection afforded to National Security Material and that afforded to Sensitive Material as specified in Table 3.1.
2. The presence of categories within classification levels is to be treated as a separate factor.

Table 4.3 Rating Scale for Exposure of Categories — National Security

Exposure of categories		
Highest data classification	**Caveats**	**Compartments**
Unclassified (U)	0	0
Restricted (R) or In-Confidence (IC)	1	0
Confidential (C) or Protected (P)	1	2
Secret (S) or Highly Protected (HP)	1	2
Top Secret (TS)	1	2

Notes

1. By definition, categories cannot exist at Unclassified level.
2. Compartments only apply to National Security Material at Confidential and above levels.
3. The factor weighting value is the same regardless of the number of categories present on the system.
4. This factor is only significant where some users are not authorised to access one or more categories present on the system.
5. Only count the most sensitive level of categories (i.e. where caveats and compartments exist on the same system then only count compartments).

4.3.1.2 Ancillary Data dependent Factors

Below are the rating tables for the ancillary data dependent factors.

Table 4.4 Rating Scale for Volume of Data

	Volume of data at highest classification level		
Highest data classification	***Low ****	***Medium***	***High *****
Unclassified (U)	0	0	0
Restricted (R) or In-Confidence (IC)	-0.25	0	0
Confidential (C) or Protected (P)	-0.25	0	0
Secret (S) or Highly Protected (HP)	0	0	0.25
Top Secret (TS)	0	0	0.25

Notes

1. This factor only applies to systems operating in Multilevel mode.
2. For data classified below Secret or Highly Protected levels, a high volume of data is not to be significant. This is due to the fact that variations from the base sensitivity value due to volume considerations are based on a proportion of the sensitivity value, being a function of the attractiveness of the data at that sensitivity level. In these cases the sensitivity value is low therefore the variations in absolute terms are considered small enough to be discounted (zero in the Unclassified case).
3. For data classified at Secret, Top Secret, or Highly Protected levels, a low volume of data is not significant. This is due to the fact that, for highly sensitive data, a low volume does not necessarily indicate a lower risk and therefore not a sufficient justification for a reduction in the base sensitivity value.
4. (*) The low volume range is intended to indicate a small portable micro-computer system. A somewhat arbitrary figure of 40 Mbytes or below is currently indicative of this type of system but this value is likely to change over time. This figure may be subject to review in borderline cases.
5. (**) The high volume range is intended to indicate a large DBMS mainframe system. A somewhat arbitrary figure of 1000 Mbytes or above is currently indicative of this type of system but this value is likely to change over time. This figure may be subject to review in borderline cases.

Table 4.5 Rating Scale for Proportion of Data

Proportion of data at highest classification level			
Highest data classification	***Low (below 10%)***	***Medium***	***High (above 80%)***
Unclassified (U)	0	0	0
Restricted (R) or In-Confidence (IC)	-0.25	0	0.25
Confidential (C) or Protected (P)	-0.25	0	0.25
Secret (S) or Highly Protected (HP)	0	0	0.25
Top Secret (TS)	0	0	0.25

Notes

1. This factor only applies to systems operating in Multilevel mode.
2. It is believed that a low proportion of data at levels above Confidential or Protected does not justify a lowering of the sensitivity rating [19].
3. It is believed that less than 10% of the data at the highest classification level is an extremely low proportion and more than 80% an extremely high proportion [19]. The range limits may be subject to review in borderline cases.

4.3.1.3 Primary User dependent Factor

Below are the rating tables for the primary user dependent factor.

Table 4.6 Rating Scale for Minimum User Clearance — DSAP

Lowest level of user clearance	
Uncleared (U)	0
Restricted (R)	1
Confidential (C)	2
Secret (S)	3
Top Secret through Negative Vetting (TS(NV))	5
Top Secret through Positive Vetting (TS(PV))	7

Notes

1. Table B.2 gives an equivalence table for US and UK clearance levels.
2. The TS(PV) level incorporates the now defunct TS(Ab) level.
3. There is no formal Restricted clearance procedure. Access to Restricted material is based on a need-to-know requirement.
4. Unless otherwise specified by and for a particular organisation, a DSAP clearance can permit the holder access to Sensitive Material in accordance with Table 3.2.

Table 4.7 Rating Scale for Maximum Data Sensitivity — PoT

Lowest level of user clearance	
Uncleared (U)	0
In-Confidence (IC)	1
Protected (P)	2
Highly Protected (HP)	3

Notes

1. The rating values apply to access to Sensitive Material only. The holder of a PoT clearance alone must not access National Security Material which is classified Confidential or above.
2. There is no formal In—Confidence clearance procedure. Access to In—Confidence material is based on a need-to-know requirement.

4.3.1.4 Ancillary User dependent Factors

Below are the rating tables for the ancillary user dependent factors.

Table 4.8 Rating Scale for Number of Users

Number of users at the lowest clearance level			
Lowest user clearance	*Low (below 10)*	*Medium*	*High (above 200)*
Uncleared (U)	-0.25	0	0.25
Restricted (R) or In-Confidence (IC)	-0.25	0	0.25
Confidential (C) or Protected (P)	-0.25	0	0.25
Secret (S) or Highly Protected (HP)	-0.25	0	0.25
Top Secret through Negative Vetting (TS(NV))	0	0	0
Top Secret through Positive Vetting (TS(PV))	0	0	0

Notes

1. This factor only applies to systems operating in Multilevel mode.
2. This factor does not apply to groups where all users are cleared and authorised to access all data on the system.
3. The low and high ranges are intended as a guide and may be subject to review in certain circumstances.

Table 4.9 Rating Scale for the Proportion of Users

Proportion of users at the lowest clearance level			
Lowest user clearance	*Low (below 10%)*	*Medium*	*High (above 80%)*
Uncleared (U)	-0.25	0	0.25
Restricted (R) or In-Confidence (IC)	-0.25	0	0.25
Confidential (C) or Protected (P)	-0.25	0	0.25
Secret (S) or Highly Protected (HP)	-0.25	0	0.25
Top Secret through Negative Vetting (TS(NV))	0	0	0
Top Secret through Positive Vetting (TS(PV))	0	0	0

Notes

1. This factor only applies to systems operating in Multilevel mode.
2. This factor applies to the proportion of users within the group. If all users in the group are cleared to the same level then clearly the factor is not applicable.
3. The range limits for the extreme values were chosen to reflect the analogous data attribute. The range limits may be subject to review in borderline cases.

4.3.1.5 System dependent Factors

Below are the rating tables for the system dependent factors.

Table 4.10 Rating Scale for Security Environment

Security Environment	
Open	0
Closed	-0.5

Note
The interpretation of the types of security environment is the same as that in the Yellow Book.

Table 4.11 Rating Scale for Terminal Type

Terminal Type	
Limited function	0
Full function - dumb	1
Full function - intelligent	2

Notes

1. For limited function, all users in the group access the system via terminals which have special limited functionality keypads which preclude the entering of direct commands.
2. For full function — dumb, all users in the group have access to the system via terminals which permit direct interactive command input sessions
3. For full function — intelligent, some users in the group have access to the system via locally programmable devices (PCs/Workstations).

Table 4.12 Rating Scale for Session Type

Session Type	
Output only	0
Transaction processing	1
Interactive	2

Notes

1. For output only, for all users in the group the system is programmed to provide predefined outputs regardless of the inputs the user presents.
2. For transaction processing, all users in the group have access to the system via transaction-based application. The application is programmed to only accept predefined, well-formed commands. All other input is rejected by the application software.
3. For interactive, some users in the group have direct access to the operating system.

Table 4.13 Rating Scale for Scope of Utilities

Scope of Utilities	
Limited	0
Full	1

Notes

1. This factor only applies to users who have some access to the operating system utilities.
2. For limited scope, access to system utilities by all users in the group is limited to non-privileged operations.
3. For full scope, some users in the group have access to a wide range of system utilities, including privileged operations.

Table 4.14 Rating Scale for External Environment

External Environment	
Hostile	0.5
Neutral	0
Benign	-0.5

Notes

1. A hostile environment is one in which it is likely that there will be at least one threat agent active on the system.
2. A neutral environment is one which has no influence on the likelihood of a threat agent active on the system.
3. A benign environment is one in which it is unlikely that there will be a threat agent active on the system.

4.3.2 Calculation of the Risk Index

The risk index is calculated using the Risk Assessment Record.

The calculation involves the following steps:

1. Calculate the Maximum Data Sensitivity rating,

   R_{max} = ***Highest level of data classification*** + ***Exposure of categories*** ratings;

2. The Minimum User Clearance rating,

   R_{min} = ***Lowest level of user clearance*** rating;

3. Calculate the sum of the data ancillary factors,

   A_{data} = ***Volume of data at highest classification level*** + ***Proportion of data at highest classification level*** ratings;

4. Calculate the sum of the user ancillary factors,

   A_{user} = ***Number of users at the lowest clearance level*** + ***Proportion of users at the lowest clearance level*** ratings

5. Calculate the Net Ancillary Factor Adjustment,

   $R_{adj} = A_{data} + A_{min}$ rounded in accordance with Table 4.15;

Table 4.15 Net Ancillary Factor Adjustment

Data/User Ancillary Factors	
$A_{data} + A_{user}$	R_{adj}
-1.00	-1
-0.75	-1
-0.50	-1
-0.25	0
0	0
0.25	0
0.50	1
0.75	1
1.00	1

Note
In the case where ancillary factors are not considered significant, set R_{adj} to 0.

6. Calculate the DERI value in accordance with Table 4.16;

Table 4.16 Data Exposure Risk Index

Data Exposure	
$R_{max} - R_{min} + R_{adj}$	*DERI value*
≤ 0	0
> 0	$R_{max} - R_{min} + R_{adj}$

7. Calculate the User Interface rating,

User Interface = Terminal Type + Session Type + Scope of Utilities ratings rounded in accordance with Table 4.17;

Table 4.17 User Interface Rating

User Interface	
Terminal Type + Session Type + Scope of Utilities ratings	*Rating*
0	-1
1 or 2	-0.5
3 or 4	0
5	0.5

Note
In the case where the User Interface factor is not considered significant set the rating to 0.

8. Calculate the System Risk value,

R_{sys} = Security Environment + User Interface + External Environment ratings rounded in accordance with Table 4.18;

Table 4.18 System Risk

System Risk	
Security Environment + User Interface + External Environment ratings	R_{sys}
-2.0 or -1.5	-2
-1.0 or -0.5	-1
0 or 0.5	0
1.0	1

9. Calculate the risk index based on the DERI with adjustment to allow for the System Risk value in accordance with Table 4.19.

Table 4.19 Overall Risk Index

Risk Index				
DERI value	R_{sys}			
	-2	*-1*	*0*	*1*
0	0	0	0	0
1	0	1	1	1
2	1	2	2	2
3	2	2	3	4
4	2	3	4	5
5	3	4	5	6
6	4	5	6	7
7	5	6	7	8
8	6	7	8	9

4.4 Determine the Overall Risk Index

After risk assessments have been carried out on all the user groups, then the overall Risk Index is taken to be the highest of the individual risk indices for each group.

4.5 Rationale for the Assessment Methodology

Assessment on a per user group basis is attributed to Landwehr and Lubbes. Landwehr and Lubbes give an example of a Sea Surface Surveillance System (S4) where two major classes of user, analysts and subscribers, are identified. "*Since analysis and subscribers are permitted different kinds of functions, have different clearances, and communicate with the S4 system over different paths, it is necessary to apply this* [risk assessment] *technique to each class of user separately.* " [5]. Furthermore, Landwehr and Lubbes consider that "*Security requirements for the system as a whole must be determined on the basis of the most risky part*" [5].

This methodology provides a measure of flexibility in the specification of the user groups. The worst case risk index from all the user groups will be no worse, but may be better, due to the moderating influence of the ancillary user factors and the user interface factors, than the risk index obtained by treating all users as a single group.

Consequently, this methodology reduces the likelihood that the overall risk will be overstated, as is the case with the Yellow Book under certain conditions, due to a more detailed analysis of the user population.

A discussion of the ratings assigned to each of the factors and the mechanisms for the combination of these ratings is given below.

4.5.1 Maximum Data Sensitivity

Unlike the Yellow Book, where the presence of categories is treated as an integral part of the data sensitivity rating, this document treats the presence of categories as a separate factor. The advantages in adopting this method are as follows:

1. the method gives a more accurate representation of the true situation in the Australian context; and
2. the method allows easy consideration of categories at any sensitivity level.

The category rating value is summed with the data sensitivity rating value to arrive at a Maximum Data Sensitivity value corresponding to the Yellow Book values under the heading "Maximum Data Sensitivity Ratings With Categories".

The rating values for the data sensitivity levels in this document are equivalent to the ratings used in the Yellow Book under the heading "Maximum Data Sensitivity Ratings Without Categories". The equivalence in values is based on the Australian and US national security data classification relationships which are specified in Appendix B.

The rating increments are linear up to the Secret level and twice the incremental value from Secret to Top Secret. *"This difference derives from the fact that the loss of Top Secret data causes exceptionally grave damage to the national security, whereas the loss of Secret data causes only serious damage* " [3].

For categories containing Secret or Top Secret data, the Yellow Book differentiates between the presence of a single category (1C) and multiple categories (MC), where the latter is considered to be twice as sensitive as the former. In the context of these guidelines, this representation has not been followed for the following reasons:

1. It is unclear whether the categories referred to in the Yellow Book at the Secret and Top Secret sensitivity levels are of the same type as the categories at the other sensitivity levels. The inference is that categories at Secret and Top Secret are SCI and at other levels are non-SCI.
2. It is believed that the type of category (caveat or compartment) is the significant feature in terms of sensitivity [16]. This reflects the strength of the special handling procedures required for each of the two types of categories which indicates that compartments are more sensitive than caveats.
3. It is believed that the distinction in terms of risk of exposure between the presence of a single category and the presence of multiple categories is not significant in the Australian context [19].

The category rating values were chosen to provide some consistency with the Yellow Book, subject to the interpretation that multiple SCI categories (MC) as defined in the Yellow Book are equivalent in risk to a compartment or number of compartments in these guidelines and all other non-SCI categories in the Yellow Book are equivalent in risk to caveats in these guidelines.
[Note: There is ***no*** equivalent in these guidelines of the one SCI category only (1C) case in the Yellow Book].

In the situation where both types of categories are present on the system then the rating is based on the category of the highest sensitivity. This is consistent with the treatment of data sensitivity levels where only the highest level is considered.

The similarity in metric scales between these guidelines and the Yellow Book facilitates the direct comparison of risk assessment methods with a view to maintaining consistency.

4.5.2 Minimum User Clearance

The rating values for the minimum user clearance levels in this document are equivalent to the ratings used in the Yellow Book up to Secret level. The equivalence in values up to Secret level is based on

the Australian and US user clearance relationships which are specified in Appendix B. Above the Secret level the ratings differ as follows:

1. The TS(NV) rating is set to 5 which is one above the Yellow Book rating for the equivalent US clearance level (TS(BI)). This overcomes the Yellow Book anomaly whereby TS(BI) clearance is sufficient to access TS classified material yet in this case the result of the Risk Index calculation (5–4=1) indicates there is a risk associated with this access. It is recognised as an anomaly by the Yellow Book in a footnote on page 5 which gives the corrected Risk Index value of 0.
2. The TS(PV) rating is set to 7 which is two above the Yellow Book rating for the equivalent US clearance level (TS(SBI)). The Yellow Book identifies two pseudo-clearance (authorisation) levels above TS(SBI) as follows:

    a. ***One Category (1C)***
    "*In addition to TS(SBI) clearance, written authorization for access to one category of information is required.*" [3], rated 6.
    b. ***Multiple Categories (MC)***
    "*In addition to TS(SBI) clearance, written authorization for access to multiple categories of information is required.*" [3], rated 7.

    There is no equivalent to this situation in the Australian context where the authorised access to categories by users does not indicate a higher overall level of trust in users, the sole measure of the level of trust being the minimum user clearance level. A user cleared to TS(PV) level, having been given the appropriate formal briefings, may be allowed regular access to a number of compartments. It is therefore considered that the level of trust afforded to these users should be equivalent to the US MC level.

The similarity in metric scales between these guidelines and the Yellow Book facilitates the direct comparison of risk assessment methods with a view to maintaining consistency.

4.5.3 Net Ancillary Factor Adjustment

The weighting values for data and user ancillary factors only apply in cases where the corresponding attribute is considered to be extreme enough to warrant a review of the DERI value and are dependent on the specific level of data sensitivity or user clearance.

The weightings have a uniform absolute value of 0.25. The reasons for this choice of value are as follows:

1. The relative importance of each of the ancillary factors is highly subjective and in terms of the DERI value are not significant. In view of this and the desire to keep the guidelines as easy to use as possible, the weighting values have been assigned uniformly.
2. It is believed that the sum of the factor weightings should never increase or reduce the DERI value by an amount greater than a single unit [16]. A choice of 0.25 with a maximum of four possible weightings produces a DERI adjustment range of ±1.0.

The calculation of the net adjustment factor is based on the following rules:

1. A combination of factor weightings is positively significant (i.e. set to 1) if the difference of the sum of the data factor weightings and the sum of the user factor weightings is > 0.25.
2. A combination of factor weightings is negatively significant (i.e. set to –1) if the difference of the sum of the data factor weightings and the sum of the user factor weightings is < –0.25.
3. A combination of factor weightings is not significant (i.e. set to 0) if the difference of the sum of the data factor weightings and the sum of the user factor weightings is in the range –0.25 to 0.25.

The calculation is based on the fact that a single attribute is considered insufficient to warrant an increase or decrease in the DERI value. However, a combination of factors may warrant an increase or decrease in the DERI value. Table 4.20 indicates the effect on the DERI of a combination of weightings.

Table 4.20 Data/User Ancillary Factor Weightings

Net DERI adjustments for ancillary factors									
	Significant Data Attributes								
Significant User Attributes	*None*	*LVD*	*HVD*	*LPD*	*HPD*	*LVD & LPD*	*LVD & HPD*	*HVD & LPD*	*HVD & HPD*
None	0	0	0	0	0	-1	0	0	+1
LVU	0	-1	0	-1	0	-1	0	0	0
HVU	0	0	+1	0	+1	0	0	0	+1
LPU	0	-1	0	-1	0	-1	0	0	0
HPU	0	0	+1	0	+1	0	0	0	+1
LVU & LPU	-1	-1	0	-1	0	-1	-1	-1	0
LVU & HPU	0	0	0	0	0	-1	0	0	+1
HVU & LPU	0	0	0	0	0	-1	0	0	+1
HVU & HPU	+1	0	+1	0	+1	0	+1	+1	+1

Legend

LVU = Low volume of users at the lowest clearance level
HVU = High volume of users at the lowest clearance level
LPU = Low proportion of users at the lowest clearance level
HPU = High proportion of users at the lowest clearance level
LVD = Low volume of data at the highest classification level
HVD = High volume of data at the highest classification level
LPD = Low proportion of data at the highest classification level
HPD = High proportion of data at the highest classification level

In contrast to DADPSWG/88–1, where ancillary factor weightings are applied at source (i.e. directly to the data and user factors before the DERI is calculated), the net adjustment factor is applied after the DERI is calculated. The reasons for this are as follows:

1. this method is easier to use where a straight Yellow Book interpretation is required (i.e. where ancillary factors are not to be considered); and
2. the application at source may result in over or under adjustments to the DERI value du to the effect of double rounding.

4.5.4 DERI Calculation

The DERI is an integer value which is a function of the Maximum Data Sensitivity, Minimum User Clearance, and Net Ancillary Factor Adjustment. The value represents the measure of "*The disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system*" [3] moderated by consideration of any extreme ancillary factor weightings.

Results of zero or less are equated to a zero value. Whereas the Yellow Book specifically adjusts the DERI value to 1 in the case where categories are present to which some users are not authorised, it is not necessary to do this in these guidelines. The adjustment is made in the Yellow Book in order to enforce the functionality requirement for mandatory access control in the case of systems operating in Compartmented mode (i.e., minimum B1 level). Since the recommended minimum ITSEC Functionality class for systems operating in Compartmented mode is F-B1 (see Table 5.1), these guidelines are consistent with the functionality requirements of the Yellow Book.

As with the Yellow Book, results of 1 or more are taken as they are.

In the case where these guidelines are to be used in the limited Yellow Book sense, then the Net Ancillary Factor Adjustment is omitted and the DERI value is directly mapped to an ITSEC assurance level.

4.5.5 System Risk Calculation

The System Risk value represents the aggregate effect of the weightings of the factors related to the system and its operating environment which are considered to be of sufficient significance to warrant a review of a minimum TCS assurance requirement based solely on the DERI value.

The process involves two levels, the calculation of the User Interface value and the calculation of the System Risk value using the result of the first operation. This hierarchic approach was adopted in order to give a choice as to the level of detail required for the measurement of the factor weightings. Consequently, if the user interface factors are not applicable to the system under review then the User Interface rating value can be set to zero without the necessity to assign values to the sub-factor weightings.

The scale of system factor weighting values is not directly related to the data and user factor values. These values have been chosen to simplify their aggregation and are not directly factored into the next level in the risk index calculation hierarchy but are translated by table.

Due to the necessary coarseness of the system risk value, some of the fidelity achieved in the summation of the weightings at both levels is lost in the table translations. This, to some extent, restricts the effect of exaggerated values due to dependencies between factors.

4.5.6 Risk Index

The Risk Index represents the DERI value, adjusted to allow for the possible influence of the System Risk factor.

The degree of influence of the System Risk factor over the DERI value is proportional to the DERI value. For the purposes of this mapping, an arbitrary figure of 20% of the DERI value for each unit of System Risk has been taken as the adjustment factor which is rounded to the nearest integer.

5 COMPUTER SECURITY REQUIREMENTS

In order to establish which trusted products/systems meet the minimum security requirements of a given computer system it is necessary to calculate the minimum levels of functionality and assurance according to the ITSEC criteria. This process is done in two stages.

1. Calculate the minimum TCS ***functionality*** level required. This involves taking into account the Mode of Operation and the specific security functionality requirements of the system and mapping onto an ITSEC Functionality Level using Table 5.1.
2. Calculate the minimum TCS ***assurance*** level required. This involves mapping the previously calculated Risk Index onto an ITSEC Evaluation Level using Table 5.2 or 5.3.

If the user wishes to ascertain the equivalent TCSEC assurance/functionality levels or the CESG assurance levels, then the equivalence tables are provided in Appendix C.

It is important to emphasise that, for systems where trusted application software products which may contain a subset of the TCB (eg. DBMS products) are to be installed, the level of trust of a system as a whole is given by the component which has the lowest evaluation level. For example, a TCS evaluated to E4 level running an MLS DBMS product evaluated to E3 level is only trusted to E3 level.
[Note: A trusted product must never bypass the security policy of the TCS on which it is running, ie, the product must be evaluated to run specifically on that TCS.]

5.1 Functionality

The COMPUSEC functionality requirements in terms of the ITSEC Functionality Classes are shown in Table 5.1.1.

Table 5.1 COMPUSEC Functionality Requirements

Minimum ITSEC Functionality Class	
Mode of Operation	***Class***
Dedicated*	F-C2
System High	F-C2
Compartmented	F-B1
Multilevel	F-B1

Notes

1. These are the minimum functionality classes required, however, the COMPUSEC requirements defined in the system security policy may dictate a higher class.
2. (*) This follows from the requirements specified in ACSI 33[20].

In addition to these minimum requirements, the functionality class must satisfy all the COMPUSEC requirements specified by the system security policy. The circumstances under which a higher functionality class (F-B2 or F-B3) is required are discussed below.

The remaining ITSEC functionality classes are not relevant to the confidentiality of the data within a system since:

- class F-IN applies to integrity of data within the system;
- class F-AV applies to availability of systems;
- class F-DI applies to integrity of data during data communications;
- class F-DC applies to confidentiality of data during data communications; and
- class F-DX applies to confidentiality and integrity of data within a computer network.

[Note: Class F–DC is addressed by COMSEC requirements, while class F-DX is indirectly addressed in Section 6 when considering limited functionality network interconnection devices].

5.1.1 Identification and Authentication

There is no increase in the Identification and Authorisation functionality between a class F-B1 system and a class F–B2 system, however, the assurance in the correct operation of Identification and Authentication is increased by the ITSEC requirement *"Identification and Authentication shall be handled by a trusted path between user and system initialised by the user."* [14].

If it is required that the trusted path be initialised by the system rather than the user then a class F-B3 is required. Such a requirement is necessary for systems where there is a risk of a subject (process) intercepting, masking, or faking a user initialised path.
[Note: This requirement is fulfilled by many commercially available MLS systems based on TCS workstations].

5.1.2 Access Control

5.1.2.1 Support of Roles

If the system must support roles in addition to users then a class F–B1 is not sufficient.

In this case, if the requirement is restricted to the roles of system operator and system administrator being performed by separate users, the class F–B2 is sufficient. If, additionally, the role of system security officer is to be performed by a separate user then a class F–B3 is necessary.

The preceding rules for the support of roles is made under the assumption that only products which fit within the specified classes are available. Of course if an evaluated product which had the appropriate functionality with the additional role mechanism was available, then it could be used. Hence it is possible for an FB-1 with the extra feature for the first case to be employed. Naturally, its defined functionality class would have to defined as something other than those currently specified by the ITSEC.

5.1.2.2 Multilevel Communication Channels

Where multilevel communication channels to attached physical devices are to operate over a range of sensitivity levels, and this range is narrower than the full range of sensitivity levels of data stored and processed on the system, then a class F–B2 is required as a minimum.

5.1.2.3 Mandatory Access Rights

Where the system is required to associate attributes (i.e. sensitivity labels) to all objects (rather than just storage objects) which are directly or indirectly accessible by subjects (e.g. ROM), then a class F–B2 is required as a minimum.

5.1.2.4 Mapping of Subjects to Objects

If the requirements specify that for each object (i.e. process, file, storage segment, or device) under discretionary access control, the system must be capable of specifying;

1. a list of all subjects (i.e. users and user groups) who have access to the object together with their mode of access, and
2. a list of all subjects who have no access to the object;

then a class F–B3 is necessary.

5.1.2.5 Multilevel Subjects

In a situation where users are accessing data of different sensitivity levels through a single interactive session, and where it is required that the user

1. be notified immediately of any change in the security level associated with that user by the subject (process) running on their behalf or the user; and
2. be able at all times to display all the subject's attributes

then a class F–B2 is required as a minimum.

5.1.3 Audit

If it is a requirement for the system to be able to audit known events which could be misused to allow an unauthorised flow of information by exploiting covert channels then a class F–B2 is required as a minimum.

Additionally, where it is required that those events which are particularly security relevant to the system as well as those events which have a critically high frequency are audited and

1. a nominated authorised user is to be informed of the occurrence of those events without delay; and
2. the system be able to initiate measures to prevent those events from further occurrence

then a class F–B3 is necessary.

5.2 Assurance

The COMPUSEC assurance requirements in terms of the ITSEC Evaluation Levels are shown in Table 5.2.

Table 5.2 COMPUSEC Assurance Requirements

Minimum ITSEC Evaluation level - Nat. Security and Sensitive Material.				
Risk Index	*Mode of Operation*			
	Dedicated	System High	Compartmented	Multilevel
0	E2*	E2	E2	E2
1	-	E3	E3	E3
2	-	-	E4	E4
3	-	-	-	E5
4	-	-	-	E6
5-9	-	-	-	**

Note

1. (*) This follows from the requirements specified in ACSI 33[20].
2. (**) The COMPUSEC security measures required to counter this level of risk are beyond that state of current technology.

5.3 Rationale for Mappings

5.3.1 Functionality

Systems operating in Dedicated mode need not rely on software functions for security requirements. However, for systems where integrity and/or denial of service requirements are specified in the security policy for the system the Yellow Book recommends a TCS class C1 as a minimum.

In the Australian context, ACSI 33 specifies that all systems should have a minimum functionality class of F-C2. This requirement clearly satisfies the weaker Yellow Book recommendation.

Systems operating in System High mode require discretionary access control only, with access to data based on a need-to-know requirement. Users of these systems must therefore be individually accountable for access to data. The functionality class F-C2 is the minimum class to provide individual accountability.

Systems operating in Compartmented mode require mandatory access control since users must have formal authorisation to access compartmented data. The data must be protected by a sensitivity label

which restricts access to only those users who are authorised to access data of that sensitivity. The functionality class F-B1 is the minimum class to provide mandatory access control.

Systems operating in Multilevel mode also require mandatory access control since users must have formal clearances and authorisation to access data. The data must be protected by a sensitivity label which restricts access to only those users who are cleared and/or authorised to access data of that sensitivity. The functionality class F–B1 is the minimum class to provide mandatory access control.

5.3.2 Assurance

In the Australian context, ACSI 33 specifies that all systems should be evaluated to at least the E2 level, regardless of the risk index. Consequently, in the situation where there is no prescribed minimum level of assurance required of the system (Risk Index is 0) an E2 evaluated system is required as a minimum. This requirement more than satisfies the Yellow Book in the circumstances under which the a minimum recommended TCSEC class is D or C1.

For users of the guidelines wishing to make a limited Yellow Book type assessment, the recommended minimum ITSEC Evaluation level is consistent with the minimum TCSEC level recommended by the Yellow Book in the same circumstances. This is based on the equivalence relationships specified in Appendix B, Allies National Security Equivalence Tables, and Appendix C.1, Mapping of ITSEC to TCSEC.

The Yellow Book distinction between the presence of a single category (1C) and the presence of a number of categories (MC) is not applicable in the Australian context. The level of assurance required to counter the risk of exposure of one category is considered to be no less strong than that required to counter the risk of exposure of a number of categories. Consequently, in cases where exposure of categories is a factor, the mapping should be equated with the Yellow Book MC case regardless of the number of categories present.

For Compartmented mode operations where some of the users are not authorised to access all the compartments, the Yellow Book recommends a class B1 system as a minimum. This recommendation is based on the functional aspects (i.e. mandatory access control) rather than the assurance aspects of this class. The recommendation for a minimum functionality class of F—B1 for all Compartmented mode operations ensures consistency with the Yellow Book.

Furthermore, the Yellow Book recommends a class B2 system as a minimum in cases where multiple compartments exist and the minimum user clearance is lower than the pseudo-level MC (see Section 4.5.2 for a definition of this level). This, in the Australian context, equates to a system operating in Compartmented mode where some users are cleared to TS(NV). In this case the guidelines are consistent with the Yellow Book (see the example specified in Appendix D.4).

In certain cases, the guidelines do not satisfy the Yellow Book requirement "*Where a system processes classified or compartmented data and some users do not have at least Confidential clearance at least a class B2 system is required*" [3] (e.g. systems operating in Multilevel security mode, processing data at a maximum sensitivity level of Confidential with lowest cleared users at Restricted level). There is no rationale in the Yellow Book for this requirement and it is unclear whether it relates to B2–specific functionality or assurance. We believe that these exceptional cases do not warrant this restriction in the Australian context.

5.4 Limitations of TCSs

When considering the use of particular classes of TCS products, it is important to appreciate the operational and procurement impacts that exist with them. The following points should be taken into account in this regard:

1. While the ITSEC is a more general standard and includes the scope of the TCSEC, the majority of TCS products have been developed according to the TCSEC standards.
2. Most commercially available products exist in the C1, C2, and B1 TCSEC classes.

3. The TCS products in the B2, B3, and A1 TCSEC classes are unique computers with limited commonality with general commercially available computers and they support a limited set of commercially available application software.

6 NETWORK CONSIDERATIONS

6.1 Introduction

The US National Computer Center Trusted Network Interpretation (TNI) [21] indicates two views for the accreditation and evaluation of a network which are dependent on the operational and technical characteristics of the environment in which the network exists. These views are summarised as follows:

1. ***Interconnected Accredited System (IAS) View***
   Parts of the network may be independently created, managed, and accredited. The network consists of multiple TCSs (components) that have been independently assigned operational sensitivity levels. Each component is accredited to handle sensitive information at either a single level or over a range of levels. The range of sensitive information that may be exchanged between two components cannot exceed the maximum sensitivity levels in common between the two components and must not give rise to a potential cascading path.
2. ***Single Trusted System View***
   A single trusted system is accredited as a single entity. The network has a single trusted computing base referred to as a Network Trusted Computing Base (NTCB) which is distributed across the network components in a manner that ensures the overall network security policy is enforced by the network as a whole.

This document is primarily concerned with the assessment of risk in networks based on interconnected accredited systems. A method for the possible reduction of overall risk by means of its confinement within logical partitions within the network is specified below. It is not, however, the intention of these guidelines to provide an algorithm for the definition of a minimal network security architecture. When designing a minimal network security architecture it is necessary to consider factors such as administrative controls, user community, network topology, and security policy. The specification of a single, generalised algorithm which encapsulates all these factors is beyond the scope of this document. These guidelines provide a set of rules for the connection of evaluated components which, if followed, will ensure that a particular network architecture presents an acceptable level of technical risk given that the appropriate physical measures are in place.

For networks based on a single trusted computing base, the risk assessment should be carried out as specified in Section 4, treating the whole network as a single distributed system. The system will then satisfy the TNI criteria at a TCSEC class which is equivalent to the minimum ITSEC evaluation level required by the guidelines.

The following terms are used in the discussions which follow.

Network Component
A component is an element in a network which performs a specific function. This functionality may range from that of a full TCS to a special limited functionality device (e.g. a LAN server). In all cases the component must have an assigned range of sensitivity levels over which data is stored and/or processed on the component and at least one direct user (this may be a system/network administrator in the case of limited functionality components). All components must possess the necessary functionality to import data from and/or export data to the network.

Component Processing Range
The range of sensitivity levels of data which is stored and processed on a component.

Component Evaluation Range
The range of sensitivity levels of data over which a component can be trusted to export data ***reliably***. This range is determined by the component's ITSEC evaluation level. The ranges are specified in Tables 6.1 or 6.2.

Communication Channel Security Functionality
The ability of a component to export/import data is determined by the component's ITSEC functionality class. Table 6.3 specifies the minimum functionality class required to support the various modes of communication between components.
Zone Processing Range
The aggregate range of sensitivity levels of data which is stored and processed within a zone[1].
Zone Evaluation Level
The evaluation level of the zone is equivalent to the level of the highest evaluated assurance component in the zone (which is the evaluation level of all components in a homogeneous zone). This level is equivalent to the Network Table Evaluation Class as specified in the TNI.

6.2 Risk Assessment in IAS Networks

The assessment of risk in networks comprising a number of independently accredited components is based on the concept of partitioning the network into a number of logical security zones.

An independently accredited component in the context of these guidelines is a component which satisfies the requirements of the guidelines in ***isolation*** (i.e., an assessment has been carried out as per Section 4 taking into account the data processed on the component and the users directly connected to the component and the resultant minimum evaluation level required is less than or equal to the evaluation level of the component).

The flow of data between zones is subject to certain conditions which are specified in Section 6.2.5. The control of inter-zone data flow is achieved by the use of special limited functionality connection devices which are described below.

The assessment procedure comprises the following steps:

1. the partitioning of the network into zones;
2. for component connections within each of the zones, the application of the specified Intra-zone connection rules and Cascading Problem Heuristic;
3. for each zone, the assessment of the aggregate risk; and
4. for connections between zones, the application of the specified Inter-zone connection rules.

Using this technique it may be possible to satisfy the requirements of the guidelines on a zone-by-zone basis and, providing the Inter-zone connection rules are satisfied, satisfy the requirements of the guidelines as a whole.

Tables 6.1 Network Component Evaluation Range Tables — National Security Material

Network Component Evaluation Ranges - National Security Material						
Minimum sensitivity level	***Maximum sensitivity level †***					
	U	**R**	**C**	**S**	**TS**	**TS + CP**
U	E2	E3	E4	E5 (E4‡)	* (E6‡)	*
R	-	E2	E3	E4	E6 (E5‡)	*
C	-	-	E2	E3	E5 (E4‡)	* (E6‡)
S	-	-	-	E2	E4	E6 (E5‡)
TS	-	-	-	-	E2	E4 (E4‡)
TS + CP	-	-	-	-	-	E2

Legend

U = Unclassified

[1] The concept of zones is discussed in a following section.

R = Restricted
C = Confidential
S = Secret
TS = Top Secret
TS + CP = Top Secret with Compartment/s

Notes

1. (†) This table gives the required component evaluation level for a given component evaluation range (maximum sensitivity level, minimum trusted sensitivity label). The maximum sensitivity level refers to the upper bound of:

   a. the range of data received from an external source in the case of a Pre-typer device operating as a receiving device (Pre-typer and Integrity Filter Devices are discussed in a later section);
   b. the exporting zone processing range in the case of an Integrity Filter device or Pre-typer device operating as an inter-zone connection device; or otherwise
   c. the component processing range.

2. (‡) These levels apply to components which have been developed and distributed in a Closed Security Environment. Otherwise, it is assumed that components have been developed and distributed in a Open Security Environment.
3. (*) The COMPUSEC security measures required to counter this level of risk are beyond the state of current technology.

Network Component Evaluation Ranges - National Security Material						
Evaluation Level	*Maximum sensitivity level †*					
	U	R	C	S	TS	TS + CP
E2	U	R	C	S	TS	TS+CP
E3	U	U	R	C	TS	TS+CP
E4	U	U	U	R	S (C‡)	TS (S‡)
E5	U	U	U	U	C (R‡)	S (C‡)
E6	U	U	U	U	R (U‡)	C (R‡)

Notes

1. The contents of the main cells in the second table refer to minimum trusted sensitivity labels as a function of component evaluation level and maximum sensitivity level.
2. (†) The maximum sensitivity level refers to the upper bound of:

   a. the range of data received from an external source in the case of a Pre-typer device operating as a receiving device;
   b. the exporting zone processing range in the case of an Integrity Filter device or Pre-typer device operating as an inter-zone connection device; or otherwise
   c. the component processing range.

3. (‡) These levels apply to components which have been developed and distributed in a Closed Security Environment. Otherwise, it is assumed that components have been developed and distributed in a Open Security Environment.

Tables 6.2 Network Component Evaluation Range Tables — Sensitive Material

Network Component Evaluation Ranges - Sensitive Material				
Minimum sensitivity level	***Maximum sensitivity level †***			
	U	**IC**	**P**	**HP**
U	E2	E3	E4	E5
IC	-	E2	E3	E4
P	-	-	E2	E3
HP	-	-	-	E2

Legend

U = Unclassified
IC = In-Confidence
P = Protected
HP = Highly Protected

Notes

1. (†) This table gives the required component evaluation level for a given component evaluation range (maximum sensitivity level, minimum trusted sensitivity level). The maximum sensitivity level refers to the upper bound of:
   a. the range of data received from an external source in the case of a Pre-typer device operating as a receiving device;
   b. the exporting zone processing range in the case of an Integrity Filter device or Pre-typer device operating as an inter-zone connection device; or otherwise
   c. the component processing range.

Network Component Evaluation Ranges - Sensitive Material				
Evaluation Level	***Maximum sensitivity level †***			
	U	**IC**	**P**	**HP**
E2	U	IC	P	HP
E3	U	U	IC	P
E4	U	U	U	IC
E5	U	U	U	U

Notes

1. The contents of the main cells in the table refer to the minimum trusted sensitivity level as a function of component evaluation level and maximum sensitivity level.
2. (†) The maximum sensitivity level refers to the upper bound of:
   a. the range of data received from an external source in the case of a Pre-typer device operating as a receiving device;
   b. the exporting zone processing range in the case of an Integrity Filter device or Pre-typer device operating as an inter-zone connection device; or otherwise
   c. the component processing range.

Table 6.3 Communication Channel Functionality

Communication Channel Functionality	
Level of Support Required	***Minimum ITSEC Functionality class***
Single-level export channels where the sensitivity level of the data transferred is implicity specified by the attribute of the channel.	F-C2
Single-level export channels where the sensitivity level of the data transferred is explicity specified and must match the attribute of the channel. Multi-level export channels where the range of sensitivities of data transferred is implicity specified by the component processing range of the export component.	F-B1
Multi-level export channels where the range of sensitivities of data transferred is explicity specified by the attributes of the channel.	F-B2*

Notes

1. These requirements are taken from the ITSEC Access Control requirements, see Section 5.1.2.2.
2. (*) For components exporting data outside the zone via a filter device, this requirement may be relaxed as the filter device may provide the necessary functionality.

6.2.1 Logical Security Zones

In this section we introduce the notion of Logical Security Zones which can confer the following benefits:

1. They provide containment of risk within zone boundaries, thus creating a barrier to the propagation of risk across a network.
2. They provide insulation from network elements outside the zone for the components (and users) inside the zone.
3. They provide a link between the computer security architecture and the physical security environment.
   [Note: This aspect is outside the scope of this document.]
4. In certain circumstances, they "break" potential Cascading Paths.

The criteria for identifying zones is dependent on a number of issues which are identified as:

- the identification of user groups;
- the relationship between user groups and data use;
- the data flow requirements;
- the security functionality requirements;
- the volume of data;
- the number of users;
- the range of data sensitivity levels;
- the range of user clearance levels; and
- the presence of categories.

Components in a zone need not be confined to a single physical location but may be geographically dispersed. An example of this is given by two networks located at separate sites and linked by a two-way secure (high-grade cryptographic) communications link. If all the components and data paths in both networks satisfy the conditions governing the definition of a valid zone (see Section 6.2.2) then the two networks and their communication link constitute a single zone.

Zones may be homogeneous (i.e. consisting of components evaluated at the same level) or heterogeneous (i.e. consisting of components evaluated at different levels). It is envisaged that most zones will be homogeneous in nature. It is recommended that the design of heterogeneous zones be avoided unless there are special circumstances which require TCSs at different evaluation levels to be connected within a zone.

Partitioning of a network into zones should be kept to a minimum due to the stringent constraints imposed on inter-zone data flow and the need for special-purpose zone interconnection devices. There is nothing to preclude the whole network being a single zone so long as the conditions governing the definition of a valid zone are satisfied (see Section 6.2.2).

As will be seen in later sections, zones are interconnected with special purpose devices such as Integrity Filters and Data Diodes.

6.2.2 Zone Partitioning

A group of interconnected network components constitute a valid zone if all the following conditions are satisfied:

1. all components within the group operate under an agreed set of compatible administrative controls;
2. all components within the group are subject to a common security policy;
3. all components within the group are linked by two-way data paths; and
4. no two components within the group are connected by a data path which is subject to manual review.

In his paper "Factors Affecting Distributive System Security" [22], Nessett argues that, in distributed systems, the assumption that each component TCB trusts all other component TCBs is dangerous due to physical security environment considerations. However, Nessett gives a proviso that the assumption is valid where the physical security environment for each component is homogeneous. The conditions required to satisfy membership of a zone (1. and 2. above) ensure that the physical security environment for each component within a zone is homogeneous and, therefore, Nessett's argument will not hold within zone boundaries.

6.2.3 Intra-Zone Connections

An intra-zone connection is defined as a two-way data path between two components in the same zone where there are no intermediate components. For convenience, this two-way connection is separated out into two "logical" one-way connections. This is done in order to allow for the possibility of asymmetric transfer of data sensitivity ranges (e.g. Component A exports data to Component B with a range U-S, Component A imports data from Component B with a range C-S).

[Note: Data paths between components and zone interconnection devices are not considered as intra-zone connections].

A component's ability to export data to and import data from other components within a zone at a single sensitivity level or over a range of sensitivity levels is dependent on the component's level of support for communication channels. This is determined by the ITSEC Functionality class of the component.

For multilevel communication channels, the range over which a component can ***reliably*** export data to another component in the same zone is dependent on the range of data sensitivity levels for which a component can be trusted to segregate and manage. This is determined by the ITSEC Evaluation level of the component.

For zones comprising two or more components, there is a potential risk of exposure resulting from the cascading problem. This problem is described in Section 6.2.3.2.

In order to ensure that the transfer, within a zone, of labeled information is reliable and the risk of exposure throughout the zone is within the limits of these Guidelines, it is necessary to apply the Intra-zone Connection Rules and the Cascading Problem Heuristic as specified below.

6.2.3.1 Rules for Intra-zone Connection

These rules are required to ensure the reliability (i.e. the integrity) of the sensitivity labels attached to data which are transferred between components within a zone. It may be argued that, since the exposure risk is contained within zone boundaries, satisfying the Cascade Heuristic for intra-zone data transfer is not necessary for the maintenance of confidentiality within a zone. However, the stronger, "TNI" label integrity condition resulting from a Cascade analysis is a requirement of these Guidelines since:

1. it provides consistency with the TNI Interconnection Rule; and
2. it ensures that, for inter-zone transfer, the importing zone can rely on the integrity of the sensitivity label of imported data, i.e. there is some level of assurance in the labelling security functionality of the component from which the data originated to assume that the data was correctly labelled.

For convenience, the rules have been categorised into those applicable to exporting components and those applicable to importing components. The onus is on the importing component to ensure that the sensitivity labels can be "believed".

6.2.3.1.1 Export of Data

The following rules apply to components exporting data to other components within the same zone and it is the exporting component's responsibility, or more precisely that component's system administrator's responsibility, to ensure that these rules are satisfied:

1. The component must have the necessary security functionality with respect to export communication channels. This can be established by reference to Table 6.3.
2. Data may be exported only at sensitivity levels which are dominated by at least one level in the target (importing) component processing range.

6.2.3.1.2 Import of Data

The following rules apply to components importing data from other components within the same zone and it is the importing component's responsibility to ensure that these rules are satisfied:

1. The component must have the necessary security functionality with respect to communication channels. This can be established by reference to Table 6.3.
2. It is the responsibility of the importing component, given knowledge of the evaluation range and processing range of the exporter, to protect its own standards of trust in labelling, by upgrading, if necessary, imported data which the importer may wish subsequently to re-export. This will imply relabelling of data whose classification dominates the minimum sensitivity level of the importer's evaluation range, but does not dominate the minimum sensitivity level of the exporter's evaluation range, to a label which does dominate the minimum sensitivity level of the exporter's evaluation range. Note that data whose sensitivity level is strictly dominated by both the exporter's and importer's evaluation levels may be freely passed, as there is an assurance that all users on both systems are cleared to see it, and that it can only leave the zone via a manual downgrading process (as with system high).

Figures 6.1, 6.2, 6.3, and 6.4 give examples of intra-zone connections.

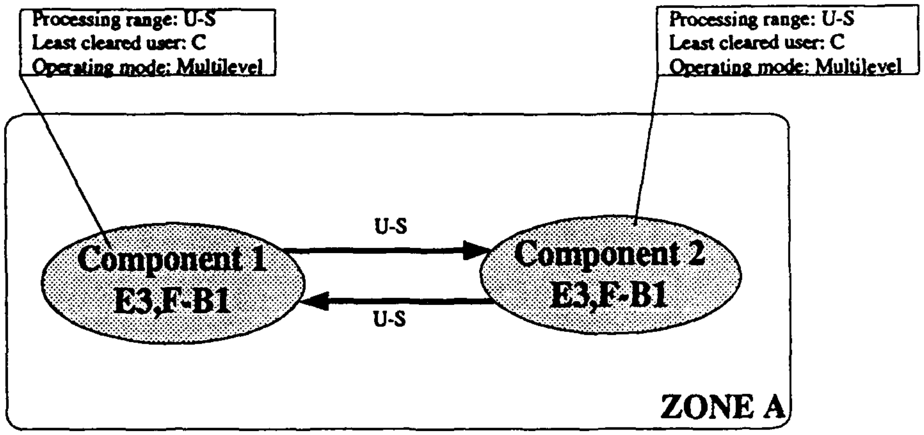


Figure 6.1 Intra-zone Connections — Example 1

Figure 6.1 represents a homogeneous zone where all components share a common processing level. In this situation, it is valid to transfer data over the whole processing range since there is no loss of confidentiality within the zone (subject to the zone aggregation considerations, see Section 6.2.4) and the sensitivity labelling is homogeneous throughout the zone.

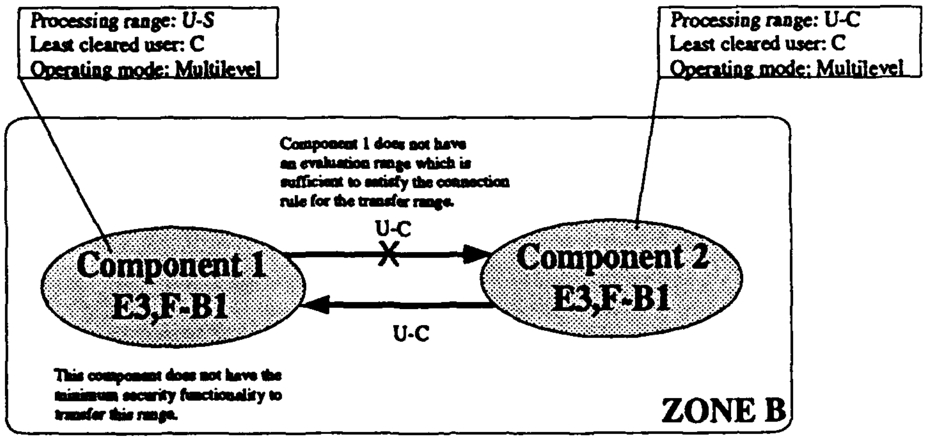


Figure 6.2 Intra-zone Connections — Example 2

Figure 6.2 represents a homogeneous zone where the intra-zone connection rules do apply. In this case there are two problems.

1. For Component 1, the data transfer range is a proper subset of the processing range. In this situation, the component must possess the ability to assign explicitly a range of sensitivities to the communication channel. The ITSEC Functionality class F-B1 does not support this level of security functionality.
2. For export of data from Component 1, its evaluation range is insufficient to give the importing Component 2 trust of data labelled at Restricted (which is within Component 2's evaluation range). Restricted data exported from Component 1 would therefore need to be relabelled Confidential to be accepted by Component 2.

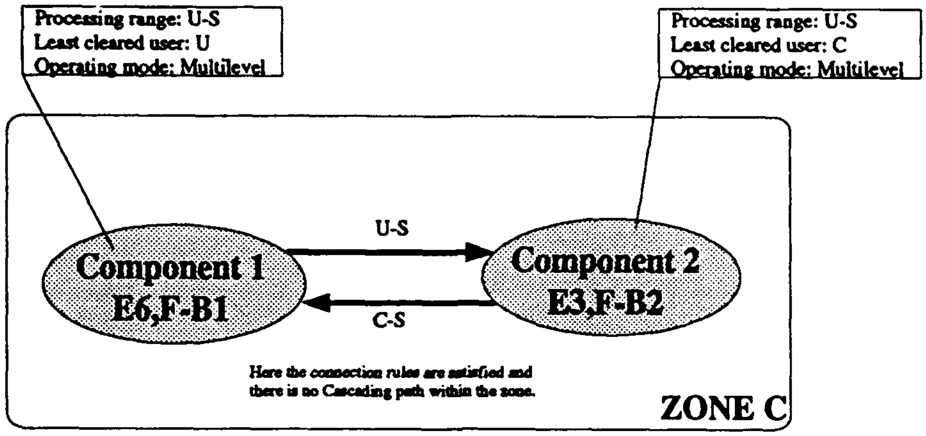


Figure 6.3 Intra-zone Connections — Example 3

Figure 6.3 represents a heterogeneous zone which satisfies the intra-zone connection rules.

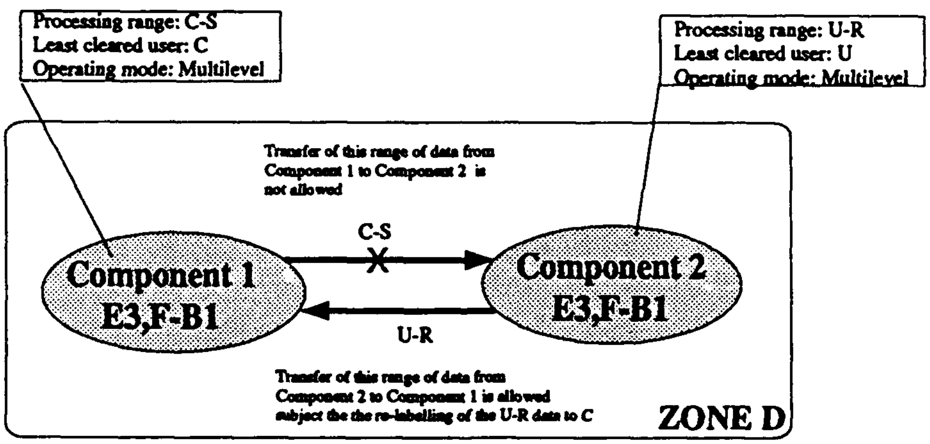


Figure 6.4 Intra-zone Connections - Example 4

Figure 6.4 represents a homogeneous zone where the components have disjoint processing ranges. The transfer from Component 1 to Component 2 is not allowed since the transfer range is not dominated by any level in the processing range of Component 2. The transfer from Component 2 to Component 1 is allowed (since the transfer range is dominated by all levels in the processing range of Component 1). However, the two components do not constitute a valid zone since only uni-directional data transfer between components is permitted. In this case the components must reside in separate zones.

All relevant intra-zone connections should be tested. If the rules are not satisfied for any connection then that data path presents an unacceptable risk and the components cannot be connected in the way specified.

6.2.3.2 Cascading Problem Heuristic

The cascading problem is described in the TNI as follows.

"*The cascading problem exists when a penetrator can take advantage of network connections to compromise information across a range of security levels that is greater than the accreditation range of any of the component systems he must defeat to do so. Cascading is possible in any connected network that processes a greater range of security levels than any one of its component systems is accredited to handle, and it is possible in others as well*" [21].

Establishing whether a cascading problem exists within a logical security zone involves the consideration of the risk of exposure along all data paths linking components within the zone. Since each individual component satisfies these Guidelines in isolation, the risk of compromise at any single component is acceptable, however, the cumulative effect of a number of compromises over several components along a particular data path may result in an unacceptable risk.

Appendix C.3.2 of the TNI specifies a number of approaches for the recognition of a potential cascade problem. The approach given in these guidelines is an adapted version of the TNI algorithm, "An Heuristic Procedure for Determining if an Interconnection Should Be Allowed".

The algorithm is based on the idea of dividing up a zone into sets of components that can potentially exchange information (i.e. send and receive data at a common sensitivity level) and are at or below a given evaluation level. The range of sensitivity levels of data which may be potentially transferred directly or indirectly between the components in the set is compared with the evaluation range for the given evaluation level to determine if the set represents an acceptable risk.

In order to assess whether there is a potential cascade problem, the procedure below should be followed.

1. A Network Security Parameters Table is produced for the zone as a whole. [Note: A proforma table is provided in Appendix A (Table A.3)].
2. If the Zone Evaluation Level is greater than the ITSEC level E3 (i.e. E4, E5, or E6), then step 3 should be followed and a Network Security Parameters Table produced for each ITSEC evaluation level below the Zone Evaluation Level down to and including E2[2].
3. Further Network Security Parameters Tables are produced by first recording any one component in the zone whose evaluation level is equal to the ITSEC evaluation level being treated. Added to the table are components which meet all of the following conditions.

    a. They have an evaluation level less than or equal to the ITSEC evaluation level being treated.
    b. They receive data from another component within the same zone at a sensitivity level that is being sent by a component which is already in the table.
    c. They send data to another component within the same zone at a sensitivity level that is equal to or less than that being received by a component which is already in the table.

    [Note: Data paths between components and zone interconnection devices should not be considered here].
    Each component at the ITSEC evaluation level being treated must be in a Network Security Parameters Table for that level. In the situation where more than one component with that evaluation level exists within the same zone and these components are linked only via a component of a higher evaluation level then a table for each of these components is required.
4. For each table, the Table Evaluation Level, the Table Maximum, and the Table Minimum should be recorded and compared, with reference to Tables 6.1 and 6.2, to establish whether the requirements of the guidelines have been satisfied.
5. If any table fails to satisfy the requirements of the guidelines then the zone presents an unacceptable level of risk and should not be connected as currently designed.

[2] Of course there must be at least one component in the zone at a given level in order to construct a Network Security Parameters Table for that level.

If the heuristic is satisfied then it can be assumed that the risk of data at a particular sensitivity level being improperly transferred to a component in the same zone which is not accredited to handle it is acceptable.

[Note: The cascade heuristic does not take into account any possible reduction in data exposure due to favorable ancillary factors. It is possible to have a situation where components satisfy the Guidelines in isolation but do not satisfy the heuristic. For this reason it is not possible to specify a general exclusion clause for the cascade heuristic (e.g. homogeneous zones in which all components have a common level of least cleared user are not guaranteed to be free of cascading paths). Conversely, no account is taken of the effect of adverse ancillary factors. However this case is covered by the aggregation effects assessment.]

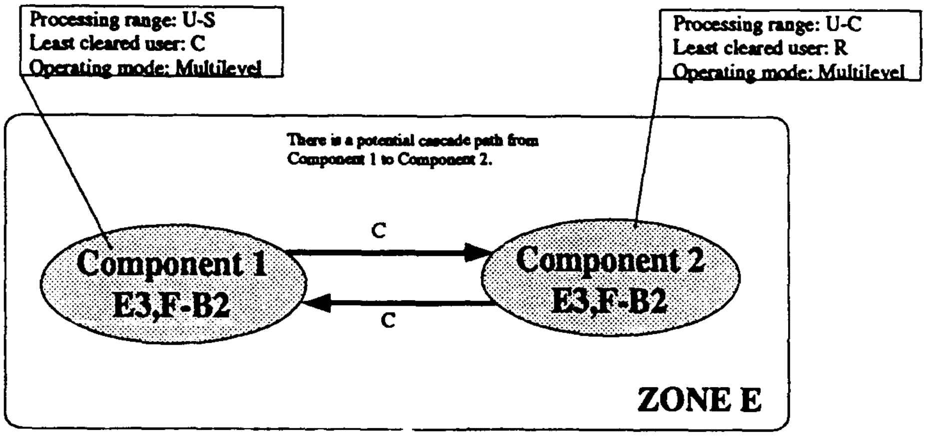


Figure 6.5 Intra-zone Connections - Example 5

Figure 6.5 gives an example of a cascading path between Component 1 and Component 2. Data classified at Secret on Component 1 may be erroneously downgraded to Confidential and transferred across the connection to Component 2. This data may then be exposed to users of Component 2 cleared only to Restricted level. For this level of risk, the Guidelines require a minimum evaluation level of E4.

6.2.4 Aggregation Effects Assessment

In order ensure that the zone evaluation level is sufficient to counter a possible increase in the risk of exposure resulting from a "blow-out" of the aggregate ancillary factors across the zone, an assessment of the significance of the aggregation effects is required.

This rule effectively precludes the arbitrary partitioning of a system which fails to satisfy the Guidelines as a single component due to high ancillary factors but may well satisfy the Guidelines when separated into a number of components. It is recognised that in certain circumstances the high ancillary factors may be restricted to a single component and that component evaluation level is sufficient to counter the resultant increase in risk. The assessment takes this possibility into account.

For each zone, the following steps should be carried out.

1. For all components in the zone which process data at the highest sensitivity level of any data in the zone, calculate the sum of the ***Volume of data at highest classification level*** factor values, S_{data}.
2. For all components in the zone which have users cleared to a level which is the lowest clearance level of any users in the zone, calculate the sum of the ***Number of users at lowest clearance level*** factor values, S_{user}.
3. Compare the values S_{data} and S_{user} with Tables 4.4 and 4.8 respectively.
4. If ***both*** values are in the ***High*** category and there is no one component within the zone for which both these factors are locally in the ***High*** category (with respect to data at the highest sensitivity and users at the lowest clearance in the zone) then the risk within the zone is unacceptable and the zone should not be connected as currently designed.

In case where the risk is unacceptable, two possible methods of reducing the risk to an acceptable level are as follows.

i. Increase the evaluation level of *every* component in the zone which has an evaluation level equal to the current zone evaluation level. [This effectively increases the zone evaluation level].
ii. Re-group the components into two or more zones where the aggregate effects of ancillary factors are no longer significant within each zone.

6.2.5 Inter-Zone Connections

An inter-zone connection is defined as a one-way data path between two components in different zones. The data flow is controlled by an intermediate limited functionality security device, which is logically isolated from both zones. This control of data flow effectively creates a barrier against the propagation of risk across zone boundaries and, in certain instances, confines the Cascading Problem within zone boundaries.

6.2.5.1 Limited Functionality Security Devices

In order to ensure limited and appropriate inter-zone data flow, certain security devices are necessary which are of limited functionality. A consequence of this limit on functionality is the fact that the device can more easily be developed to be highly trusted, thus providing a more cost effective countermeasure.

6.2.5.1.1 Data Diode

The security function of a data diode is to allow data to flow in only one direction so as to ensure confidentiality.

A data diode may be used to help ensure integrity through the device having additional properties which check on various attributes of the data which is transferred. For example, the diode may pass only documents which satisfy a given format, or only those containing characters of a given alphabet. The main reason for this checking is to help prevent the introduction of viruses and other data which may have a purpose other than that permitted.

If a data diode finds data which does not satisfy its given criteria, it may re-route the information to a dedicated device or machine for checking.

The data diode is a device which falls into the ITSEC Functionality Class F-DX.

6.2.5.1.2 Classification Integrity Filter

A classification integrity filter performs a security function equivalent to enforced manual review of the classification of data prior to its transfer. Because of this, the integrity filter is useful in allowing data to be passed outside a zone in circumstances where the zone carries data of a classification such that, with the level of trust present in the computers used within the zone, the risk of passing the data outside the zone would otherwise be considered too high. The effectiveness of the filter is derived from its ability to transfer the review process back to the originator of information in such a manner that the "man in the middle" solution becomes unnecessary.

(A data diode is a counterpart of the classification integrity filter in that it provides a mechanism to allow input of data to a zone without allowing output of data from the zone to bypass the integrity filter.)

The enforced manual review procedure within an integrity filter acts as a break in the data paths between components in the sending zone and components in the receiving zone and, as such, restricts the Cascading Problem to within the sending zone.

The risks involved in the output of data classified below the applicable component evaluation range for a particular class of TCS without manual review were identified in the Yellow Book. Essentially, the

risks arise because the recipients of the data are considered as indirect users of the system which permits the export of data without manual review.

An integrity filter, when certified as being highly trusted, can reduce unacceptable levels of risk in these circumstances. The maximum range of data sensitivity levels over which the device can be trusted to operate is determined by its evaluation level (see Tables 6.1 and 6.2.).

The operation of a classification integrity filter consists of two parts.

1. When there is a requirement to transfer data, the data is displayed to an authorised user for review via an effective trusted path to ensure that the correct classification has been applied.
2. Following the manual review, the transfer can be performed via an effective trusted path.

If a delay is necessary between the two operations, then the reviewed data and its correct classification may be "sealed" by applying a cryptographic checksum which can be decoded by the integrity filter. The second operation may be performed some time later when the decoding of the checksum confirms that neither the data nor the classification has been changed since the manual review took place.

The classification integrity filter is a device which falls into the ITSEC Functionality Class F-DX.

6.2.5.1.3 Pre-typer

A pre-typer is a device which is similar to the integrity filter except that the manual review operation is superseded by a pre-determined automatic application of a sensitivity label. This functionality is necessary in cases where a high data bandwidth makes human review procedures impractical.

The operation of the pre-typer consists of two modes:

1. Data imported from an external source has a pre-determined sensitivity label automatically applied by the device according to the source of the data. The sensitivity label is "sealed" by applying a cryptographic checksum which can be decoded by the pre-typer and the data is transferred to the initial receiving zone via an effective trusted path.
2. When there is a requirement to export the "sealed" data from the initial receiving zone to another zone within a network, possibly via a number of intermediate zones, each zone along the path of the "sealed" data must be connected to its immediate neighbour by a pre-typer device which performs the following functions:

   a. checks the integrity of the label; and
   b. controls the transfer of "sealed" data to the neighbouring zone in accordance with the security policy.

   If the label is intact and the transfer is permitted then the transfer is performed via an effective trusted path.

The pre-typer is a device which falls into the ITSEC Functionality Class F-DX.

6.2.5.2 Rules for Inter-Zone Connection

These rules are required for the following reasons:

1. to ensure that data at a particular sensitivity level is transferred only to zones which are able to process that level;
2. to ensure that the importing zone can rely on the integrity of the sensitivity label attached to data transferred from the exporting zone;
3. to control the cascading problem between zones; and
4. to preclude data leakage via covert channels from a zone processing highly sensitive data to a zone processing less sensitive data.

The rules for connection of network zones are dependent on the characteristics of the sending zone, receiving zone, and the data path between the zones. The Inter-zone Data Flow Table in Appendix A.2 can be used to facilitate the testing for compliance with these rules.

6.2.5.2.1 General Rules

The following rules apply to all inter-zone connections regardless of the type of connection.

1. For heterogeneous zones, only components evaluated to the same level as the zone evaluation level may directly export data to or directly import data from another zone. This rule ensures that only those components which have an evaluation level sufficient to process data at the highest level of sensitivity in the zone and to support the least cleared user of the zone without risk are allowed to export and import data. As a consequence, the export or import component is representative of the zone as a whole with respect to transfer ranges and minimum user clearance conditions.
2. All data paths between zones are considered to be one-way only (i.e. no acknowledgments). [This rule does not preclude data transfer between zones in both directions, however, the data paths are to be considered as two logically separate one-way connections]. This rule helps prevent covert channels between the receiving zone and the sending zone.
3. The importing component can receive only data at a level which is dominated by at least one level within its component processing range.
   [If the level of the imported data is dominated by at least one level in the importing component processing range but is outside the range then the imported data must be re-labelled upon reception at a single level which is the lower bound of the importing component processing range]. This rule ensures that only those zones which are trusted to process this level of data are allowed to import.
4. Both the exporting and importing components must have the necessary security functionality with respect to the type of communication channel. This can be established by reference to Table 6.3. This rule ensures that the transfer is functionally achievable.
5. If the required level of assurance for the zone interconnection is greater than or equal to E6, then a "spooling" output to integrity filters[3] is required to reduce the possible effect of covert channels[4].

6.2.5.2.2 Functionality devices

The remaining rules specifically relate to the type of connection and are specified below.

6.2.5.2.2.1 Data Diode

In general, where it is required to transfer data to a zone processing highly sensitive data from a zone processing less sensitive data, a data diode should be used.

Data may be transferred between two components in different zones via a data diode device subject to the following conditions.

1. The sending zone processing range is dominated by the clearance level of the least cleared user in the receiving zone. This rule effectively restricts consideration of the cascading problem to within zone boundaries since all users in the receiving zone are cleared to access the entire range of sensitivity levels of data processed on the sending zone.
2. The evaluation level of the device is sufficient to assure that the bandwidth of the potential covert channel resulting from leakage of data from the receiving component to the sending component is below an accepted maximum. It is recommended that the device be evaluated to at least level E6.

---

[3] See following sections.

[4] See also "Stubs: An Overview" by Anderson et al (ERL Research Report, Salisbury, 1992) for explanation concerning spooling output and covert channels.

Subject to the above conditions, the sending zone may transfer data over its entire processing range. Figure 6.6 illustrates the application of these rules.

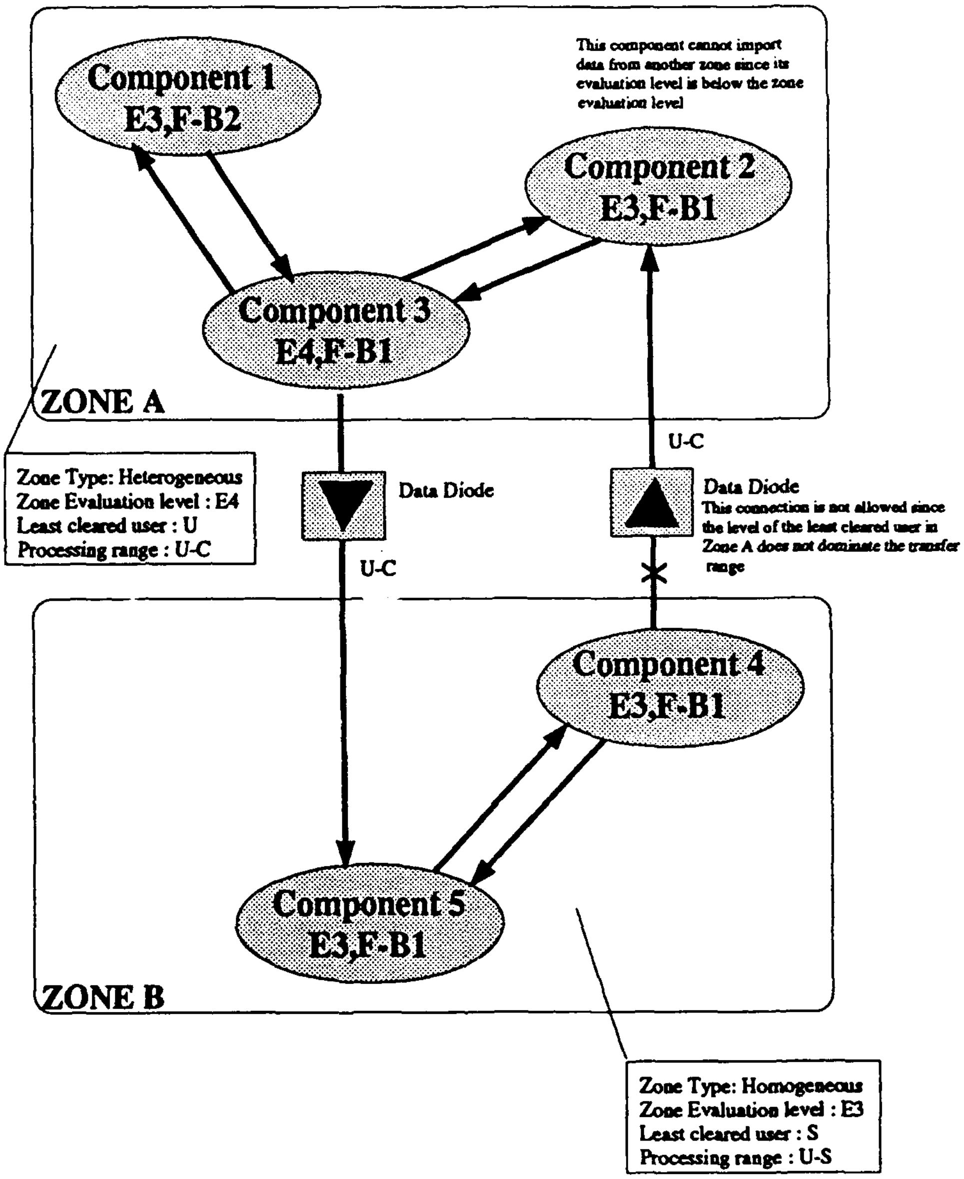


Figure 6.6 Inter-zone Connections - Example 1

6.2.5.2.2.2 Integrity Filter

Where it is required to transfer data between components in different zones in which the range of sensitivity levels is such that the importing component cannot rely on the exporting component to label this range correctly, an integrity filter should be used.

Data may be transferred between two components in different zones via an integrity filter device subject to the following conditions.

1. The range of sensitivity levels over which the device can be trusted to transfer data correctly is bounded by its evaluation range. The evaluation range is a function of the evaluation level of the device and is determined by reference to Tables 6.1 and 6.2.

2. The evaluation level of each integrity filter along a data path must be sufficient to counter the risk of exposure due to a potential cascading problem along that path. That is, the evaluation range must contain the range covering the lowest clearance level of all users in the zones along the data path up to the highest sensitivity level of data in the sending zone.

Figure 6.7 illustrates the application of this rule.

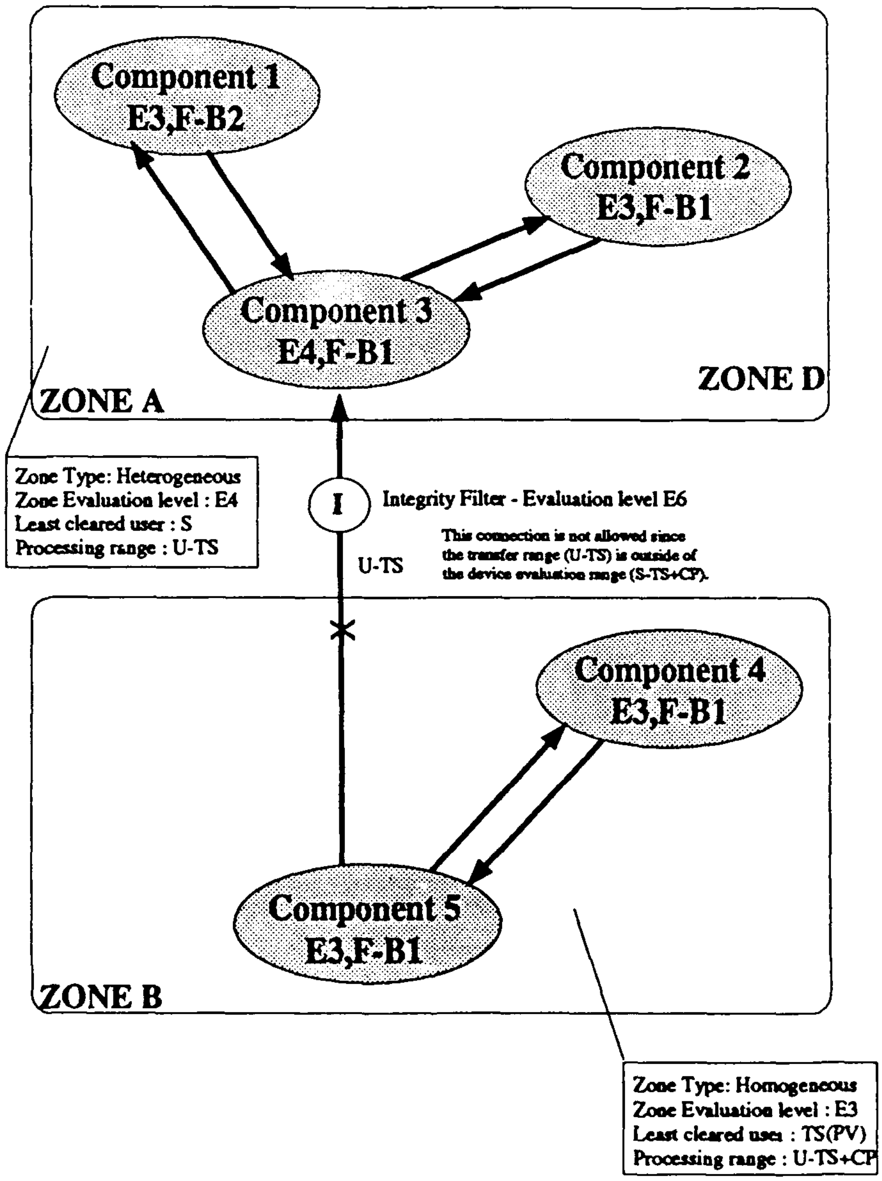


Figure 6.7 Inter-zone Connections - Example 2

6.2.5.2.2.3 Pre-typer

Data may be transferred between different zones via a pre-typer devices subject to the following conditions.

1. The range of sensitivity levels over which the device can be trusted to correctly transfer data is bounded by its evaluation range. The evaluation range is a function of the evaluation level of the device and is determined by reference to Tables 6.1 and 6.2.
2. All inter-zone connections along data paths where "pre-typed" data is being transferred must be linked by pre-typer devices of the same evaluation level which is the evaluation level required of the initial receiving pre-typer.
3. The evaluation level of each pre-typer device along a data path must be sufficient to counter the risk of exposure due to a potential cascading problem along that path. That is, the evaluation range must contain the range covering the lowest clearance level of all users in all the zones along the data path up to the highest sensitivity level of data received from the external source.

Figure 6.8 illustrates the application of these rules.

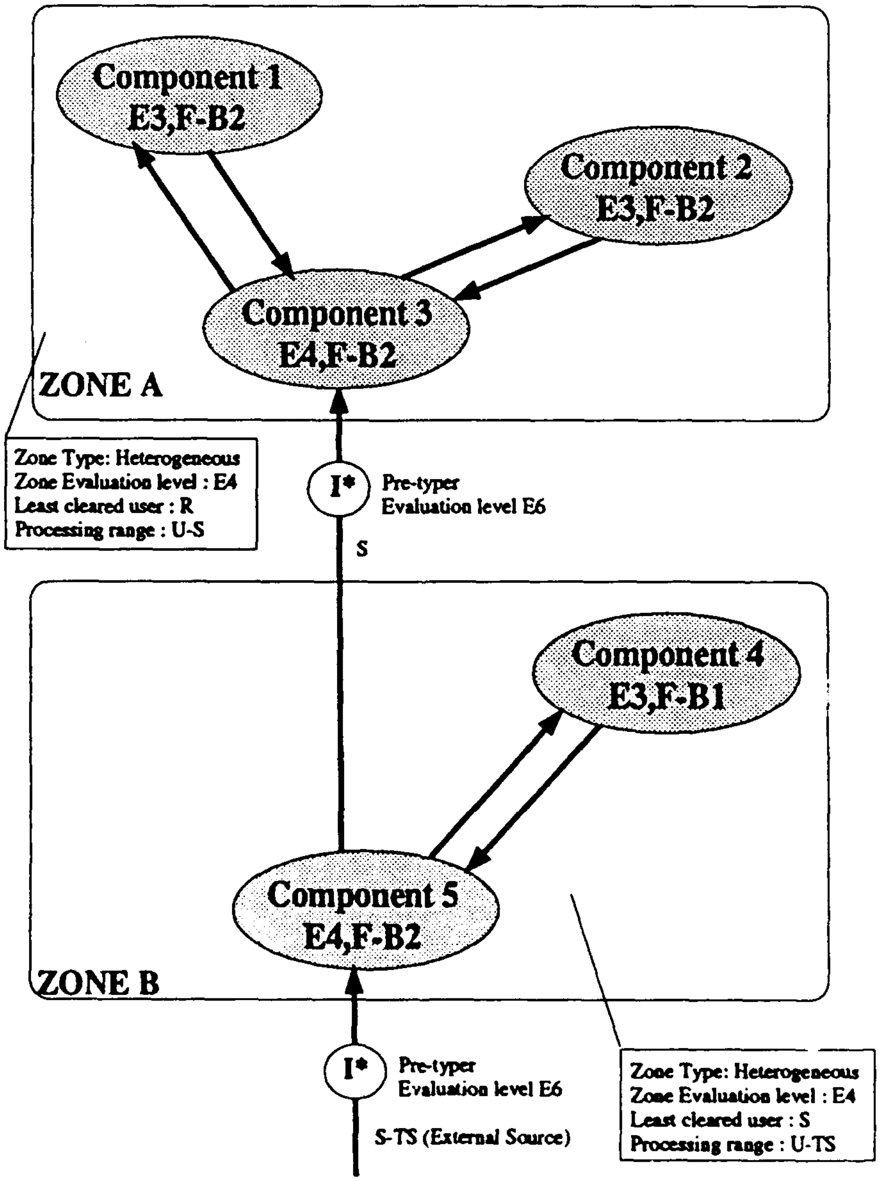


Figure 6.8 Inter-zone Connections - Example 3

Figure 6.9 provides an example of a situation where there does exist an inter-zone cascading problem.

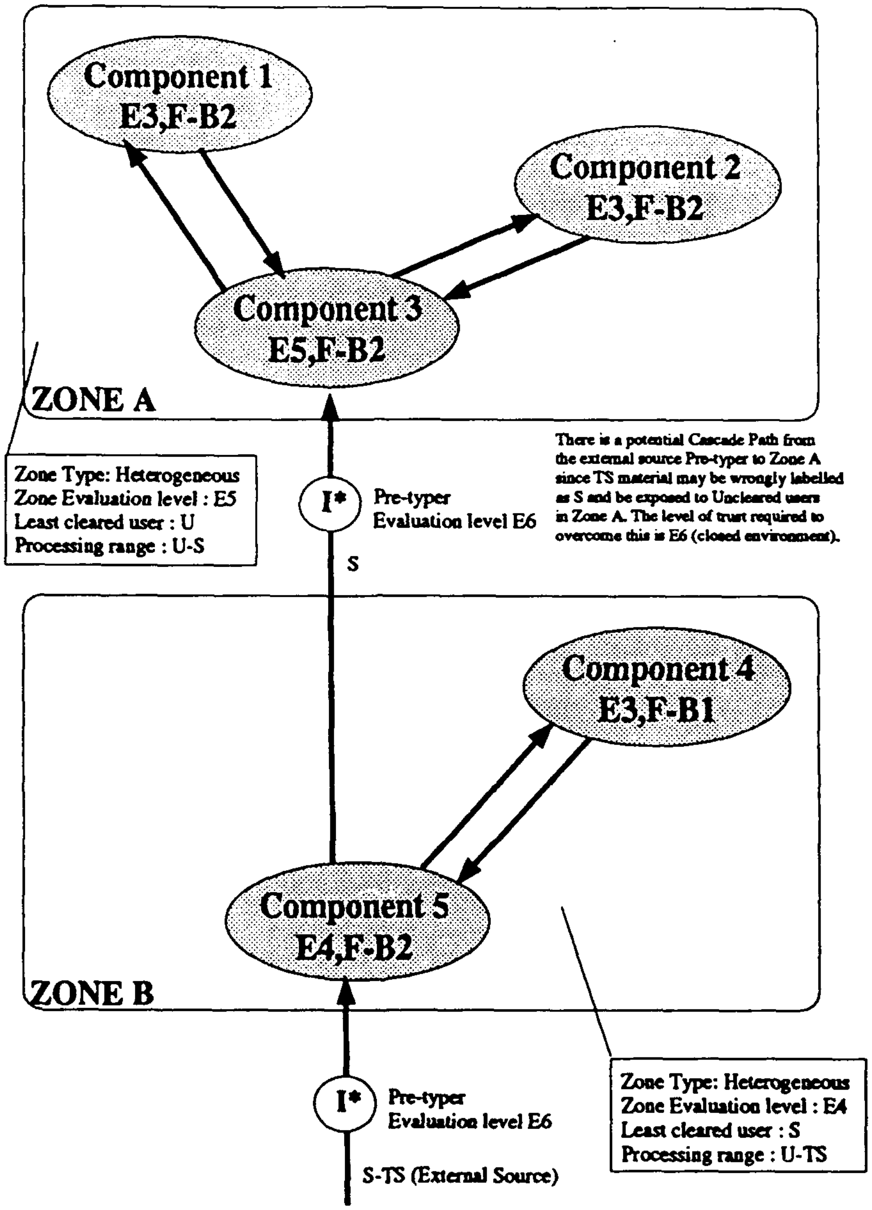


Figure 6.9 Inter-zone Connections - Example 4

6.2.5.2.2.4 Manual review

Data may be transferred between two components in different zones by non-electronic means (i.e. where the data is in the form of a limited alphabet representation, e.g. printed matter) if an authorised user performs a review of the sensitivity label, prior to transfer, to ensure that the correct sensitivity label has been applied. This effectively eliminates the risk of a component electronically applying an improper sensitivity label to data which is to be exported to another component. The transfer is subject to the following condition:

1. The sensitivity range of the data to be transferred must be within the processing range of the receiving zone.

6.2.5.2.2.5 Transfer of Data via Removable Media

Data which is transferred between zones ***without manual review*** via removable media (e.g. printed matter, magnetic tape, removable disk) is subject to similar rules to those covering the diode.

1. The range of sensitivity levels of data transferred to removable media must be bounded by the component evaluation range of the ***exporting*** component. The upper bound of the component evaluation range is the highest sensitivity level of data residing on the ***exporting*** component. The lower bound of the component evaluation range is a function of the component evaluation level and is determined by reference to Tables 6.1 and 6.2.
2. The sending zone processing range is dominated by the clearance level of the least cleared user in the receiving zone. This rule effectively restricts consideration of the cascading problem within zone boundaries since all users in the receiving zone are cleared to access the entire range of sensitivity levels of data processed on the sending zone.

Note that the general rule covering heterogenous zones applies in this case. Only components evaluated to the same level as the zone evaluation level may directly export data to or directly import data from another zone. This means that devices which read from and write to removable media must be located on the highest evaluated component in the zone.

7 ACKNOWLEDGMENTS

Mr. Greg Royle is acknowledged for his input in earlier versions of these guidelines and for the background information supplied on measuring the exposure of data categories. The Department of Defence EIP Branch is acknowledged for funding the production of a set of trusted system guidelines for both defence and civilian government environments. Mr. John Rogers of the Defence Signals Directorate, Mr. Bill MacCallum and Mr. Colin Hale of the Defence Security Branch, and Dr. Malcolm Stevens of the Trusted Computer Systems group are thanked for their comments and background information which greatly assisted in the production of this document.

8 GLOSSARY

****-property***
A rule of the Bell & La Padula security model which prevents the occurrence of "write-downs" (i.e. where a subject writes to an object which has a lower sensitivity level than that of the subject).

Access
Refers to access to data through either:

- a terminal connected to the system; or
- another computer system; or
- external media (i.e., hardcopy, removable disk, magnetic tape, etc) where no manual review is required.

Assets
Assets include both the information processed by a computer system and the system itself. This document is concerned with the informational assets which have a value to the owner or user of the system. The value of an asset is a measure of its worth to the owner.

Availability
Refers to the security requirement whereby information and resources can be accessed by authorised users when required.

Cascading Problem
For a network of component systems, the cascading problem exists when a penetrator can take advantage of network connections to compromise information across a range of sensitivity levels that is greater than the evaluation range of any of the component systems he must defeat to do so.

Category
The term category in the context of this document refers to all data whose access, over-and-above the normal clearance restrictions, is subject to special handling conditions.
Caveat
Categories which may be accessed by a specified group of subjects and/or under specified circumstances for which no special briefing is required. Caveats may be characterised into the following types:

- awareness — the labelling of data with warning caveats (e.g. WNINTEL);
- extensive — the extension of releasability to a set of subjects (e.g. releasability indicators); and
- restrictive — the restricting of distribution to a set of subjects (e.g. AUSTEO).

Closed Security Environment
A security environment is closed if both of the following conditions holds true:

- application developers (including maintainers) have sufficient clearance and authorisations to provide an acceptable presumption that they have not introduced malicious logic; and
- configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.

Communication Channel Security Functionality
The ability of a component to export/import data is determined by the component's ITSEC functionality class. Table 6.3 specifies the minimum functionality class required to support the various modes of communication between components.
Compartment
Categories which may be accessed only by subjects who have received a special briefing covering the handling of this material. Compartments are always restrictive.
Compartmented Security Mode
A mode of operation which allows the system process two or more types of compartmented information (information requiring a special authorisation) or any one type of compartmented information with other than compartmented information. In this mode, the system access is secured to at least Top Secret (TS) level, but all system users need not necessarily be formally authorized access to all types of compartmented information being processed and/or stored in the system.
Compromise
The possible degradation to the security of an asset from a defined acceptable level.
Confidentiality
Refers to the security requirement whereby information should only be disclosed to those users who are authorised to access that information.
Covert Channel
An unintended communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy.
Countermeasure
See Safeguard.
Data
For the purposes of COMPUSEC, this term refers to information, documentation, or software which is stored and/or processed on a computer system.
Data Exposure
The impact caused by the unauthorised disclosure of information.
Dedicated Security Mode
A mode of operation where a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period.
Denial of Service
Action or actions which prevent any part of the system from functioning in accordance with

its intended purpose. This includes any action which causes the unauthorised destruction modification, or delay of service.

Direct Users

These are persons authorised to have direct access to data via a terminal connected to the system

Discretionary Access Control

A method of restricting access to data by subjects based on the identity and the "need-to-know" requirements of the subject. The rules governing this type of access are discretionary insofar as certain users are given the discretion of granting access to specific objects by specific subjects.

Evaluation Level

The level of assurance afforded to a TCS with respect to the correct operation of its security functions.

Impact

See Threat Effects.

Indirect Users

These are persons authorised to have indirect access to data transferred via another computer system electronically connected to the system or removable media (i.e., hardcopy, removable disk, magnetic tape, etc) where no manual review has been performed

Integrity

Refers to the security requirement whereby information is being handled as intended and has not been exposed to accidental or malicious alteration or destruction.

Limited Functionality Connection Devices

These devices are specifically designed to support the use of logical security zones, controlling the data flow between zones. A consequence of this limit on functionality is the fact that the device can more easily be developed to be highly trusted. Examples of these types of device are integrity filters and data diodes.

Logical Security Zone

A zone comprises a set of one or more components that, between themselves, can potentially exchange information in both directions, ie send and receive data at a common sensitivity level, and have an evaluation class at or below a given level. The use of zones effectively provides containment of risk by limiting the flow of data between each zone. This control of inter-zone data flow is achieved by the use of special limited functionality connection devices. The word logical is used to imply the fact that a zone can be geographically a dispersed entity.

Logical Security Zone Evaluation Level

The evaluation level of the zone is equivalent to the level of the highest evaluated component in the zone (which is the evaluation level of all components in a homogeneous zone). This level is equivalent to the Network Table Evaluation Class as specified in the TNI.

Logical Security Zone Processing Range

The aggregate range of sensitivity levels of data which is stored and processed within a zone.

Malicious Logic

Software, firmware, and/or hardware which is deliberately introduced into a computer system for the purpose of compromising the system.

Mandatory Access Control

A security policy which restricts the access to sensitive material by subjects based on a the granting of a formal authorisation (i.e. clearance, and/or briefings) to the subject to access the sensitive material.

Manual Review

Manual review is the activity carried out by an authorised person which ensures that the sensitivity label of the data being reviewed accurately reflects the contents of the data.

Multilevel Device

A device that is trusted to simultaneously process data of two or more sensitivity levels without compromise.

Multilevel Security Mode

A mode of operation which allows two or more classification levels of information to be

processed simultaneously within the same system when some users are not cleared for all levels of information present.

Network Component

A component is an element in a network which performs a specific function. This functionality may range from that of a full TCS to a special limited functionality device (e.g. a LAN server). In all cases the component must have an assigned range of sensitivity levels over which data is stored and/or processed on the component and at least one direct user of the component (this may be a system/network administrator in the case of limited functionality components). All components must possess the necessary functionality to import data from and/or export data to the network.

Network Component Evaluation Range

The range of sensitivity levels of data over which a component can be trusted to *reliably* export data. This range is determined by the component's ITSEC evaluation level. The ranges are specified in Tables 6.1 or 6.2.

Network Component Processing Range

The range of sensitivity levels of data which is stored and processed on a component.

Object

A term used in security modelling to describe a container of information. The object may be a storage item (record, block, sector, file, directory, etc.), a memory item (page, segment, etc.), or a device (terminal, printer, etc.).

Open Security Environment

A security environment is open if either of the following conditions holds true:

- application developers (including maintainers) do not have sufficient clearance (or authorisation) to provide an acceptable presumption that they have not introduced malicious logic; or
- configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications.

Process

A program which is in an execute state.

Risk Analysis

The identification of specific system assets, the threats to these assets, the system's vulnerability to these threats, and the identification and cost of the safeguards necessary to counter these threats.

Risk Assessment

The comprehensive determination of the state of risk associated with a system based upon a risk analysis.

Risk Index

This is a term taken from the Yellow Book and is a measurement of the degree of mis-match between the highest classification level of information processed on a system and the lowest clearance level of users of that system.

Risk Management

The combination of risk assessment, management decision, and control implementation. The process involves the decision on how to most effectively reduce risks to system assets where the assessed risk exceeds a given level of acceptability. This may involve cost/benefit analysis of the safeguards required to reduce risks.

Safeguards (Countermeasures)

The measures that protect assets from compromise by virtue of the safeguard's physical, logical, and procedural characteristics. Safeguards may be categorised as physical, administrative, procedural, communications (COMSEC), and computer system (COMPUSEC). Examples of COMPUSEC safeguards include:

- trusted systems;
- trusted application or support software;
- trusted communication pathways; and

- trusted support hardware.

Guidance on the use of safeguards in other categories is provided in SECMAN 3. A system is only considered secure when necessary safeguards from all categories are implemented.

Single-level Device

A device which is trusted to process data at only one sensitivity level. This includes devices which may process data at different sensitivity levels but not concurrently.

Subject

A term used in security modelling to describe an entity which causes information flow among objects. The subject may be a user, a process, or a device.

System High Security Mode

All system users in this environment possess clearances and authorizations for all information contained in the system but some users do not have need-to-know access to all information. The system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.

Threats

These are active forces posing some danger or menace to the assets. Threats may be people (threat agents), occurrences, or entities that can compromise an asset's security.

Threat Agents

This is the perpetrator of a threat. Threat agents can be either human or environmental. The measure of threat to an asset by a human agent is a function of the assets' attractiveness to the agent, the motivation and capabilities of the agent, and the opportunities available to the agent. The possible goals of the threat agent which are related to confidentiality are as follows: to disclose data to interested individuals, foreign powers, press, competition, government agencies, or to gain access to data (disclose to self).

Threat Effects (Impacts)

Potentially harmful outcomes of an action by a threat agent on the informational assets of a computer system. The types of impact are as follows:

- exposure of data;
- corruption of data (including destruction); and
- denial of service.

Trusted Computing Base

The collection of software, firmware, and/or hardware which perform the security functions necessary to enforce the security policy of a computer system.

Trusted Path

A software, firmware, and/or hardware feature which permits a user to communicate directly with the TCB. The path is initialised either by the user or the TCB.

Users

For the purposes of COMPUSEC, this term refers to humans who are authorised to have access to some or all of the data residing on a computer system.

Vulnerability

The level of susceptibility of a system (and thereby the informational assets it processes) to compromise.

9 LIST OF ABBREVIATIONS

1C	One Category
Ab	Absolute
ACSI	Australian Communications-Electronic Security Instruction
ADP	Automatic Data Processing
AIS	Automated Information System
ALE	Annualised Loss Expectancy
ANSSR	Analysis of Networked Systems Security Risks
AUSTEO	Australian Eyes Only
BI	Background Investigation
C	Confidential
CCTA	Central Computer and Telecommunications Agency (UK)
CESG	Communications - Electronics Security Group (UK)
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CRAMM	CCTA Risk Analysis and Management Methodology
DADPSWG	Defence ADP Security Working Group (UK)
DBMS	Data Base Management System
DERI	Data Exposure Risk Index
DoD	Department of Defense
DSAP	Designated Security Assessment Position
DSB	Defence Security Branch
EPV	Enhanced Positive Vetting
ERM	Effective Risk Management
GCHQ	Government Communications Headquarters (UK)
GENSER	General Service
HP	Highly Protected
IAS	Interconnected Accredited System
IC	In-Confidence
ITSEC	Information Technology Security Evaluation Criteria
LAVA	Los Alamos Vulnerability/Risk Assessment
MBytes	Megabytes
MC	Multiple Categories
N	Not Cleared but Authorised Access to Sensitive Unclassified Information or Not Classified but Sensitive
NBS	National Bureau of Standards (US)
NCSC	National Computer Security Center (US)

NTCB	Network TCB
NV	Negative Vetting
P	Protected
PC	Personal Computer
PoT	Position of Trust
PSM	Protective Security Manual
PV	Positive Vetting
R	Restricted
ROM	Read-only Memory
S	Secret
S4	Sea Surface Surveillance System
SBI	Special Background Investigation
SCI	Sensitive Compartmented Information
SECMAN 3	Computer System Security Manual†
SOL	Single Occurrence of Loss
SQL	Structured Query Language
TCB	Trusted Computing Base
TCS	Trusted Computer System
TCSEC	Trusted Computer System Evaluation Criteria
TNI	Trusted Network Interpretation
TS	Top Secret
U	Unclassified or Uncleared
UK	United Kingdom
US	United States
WNINTEL	Warning Notice - Intelligence Sources and Methods Involved

† SECMAN3: System Information Security Manual, Edition 4, Department of Defence. 1991.

REFERENCES

[1] Attorney-General's Department. *Protective Security Manual.*

[2] National Computer Security Center. *Computer Security Requirements — Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-003-85*, June 1985.

[3] National Computer Security Center. *Technical Rationale Behind CSC-STD-003-85: Computer Security RequirementsGuide for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85*, June 1985.

[4] US Department of Defense. *Trusted Computer System Evaluation Criteria, DoD 5200.28--STD*, December 1985.

[5] C.E. Landwehr and H.O. Lubbes. Determining Security Requirements for Complex Systems with the Orange Book. In *Proceedings of the 8th NBS/NCSC National Computer Security Conference, pp 156-162*, September 1985.

[6] Defence Security Co-ordinating Committee. *Ministry of Defence Computer Security Requirements in Specific Environments, DADPSWG/88-1*, January 1988.

[7] LOGICON, Inc. *A Guide to Effective Risk Management: Decision Support System*, version 2.5 edition, September 1989.

[8] D.J. Bodeau, F.N. Chase, and S.G. Kass. ANSSR: A Tool for Risk Analysis in Networked Systems. In *Proceedings of the 13th NIST/NCSC National Computer Security Conference, pp 687-696*, 1990.

[9] US Department of Commerce, National Bureau of Standards. *Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65*, August 1979.

[10] R.H. Jr. Courtney. *Security Risk Assessment in Electronic Data Processing Systems.* IBM Systems Research Center, New York, December 1975.

[11] Mosleh A. A Matrix/Bayesian Approach to Risk Management of Information Systems. In *Proceedings of the Computer Security Risk Management Model Builders Workshop, pp 103-116*, May 1988.

[12] BIS Applied Systems UK Ltd. *CCTA Risk Management in Computer Systems and Networks*, 1986.

[13] Los Alamos National Laboratory. *LAVA for Computer Security: An Application of the Los Alamos Vulnerability Assessment Methodology, Release Version 1.01, LA-UR-86-2942*, September 1987.

[14] Harmonised Criteria of France-Germany-the Netherlands-the United Kingdom. *Information Technology Security Evaluation Criteria*, 10 January 1991. Version 1.1.

[15] Government Communications Headquarters. *CESG Computer Security Memorandum No. 3, UK Systems Security Confidence Levels*, February 1989.

[16] Record of Conversation between ITD and DSB, Canberra, 17 Jan 1991.

[17] The Computer Security Threat to Navy SCI Systems. LOGICON, Inc., 1988.

[18] D.E. Bell and L.J. La Padula. *Secure Computer Systems: Mathematical Foundations and Model.* Mitre Corporation, Bedford Mass., 1973.

[19] Record of Conversation between ITD and DSB, Salisbury, 24 Jan 1991.

[20] Defence Signals Directorate. *ACSI 33.* in preparation.

[21] National Computer Security Center. *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005*, July 1987.

[22] D.M. Nessett. Factors Affecting Distributed System Security. In *Proceedings of the IEEE Symposium on Security and Privacy, pp 204-222*, May 1986.

APPENDIX

APPENDIX A RISK ASSESSMENT TABLES

A.1 Security Parameters

Table A.1 provides a checklist of parameters required to carry out a risk assessment.

Table A.1 Security Parameters Record

Security Parameters Record		
System Identity		
Evaluation level		
User Group Identity		
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	
Most sensitive category type	*Caveat, Compartment, None*	
Total volume of data	*MBytes*	
Volume of data at the maximum sensitivity level	*MBytes*	
Total number of users in the group	*1 to N*	
Number of users at the minimum clearance level	*1 to N*	
Security environment type	*Open, Closed*	
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	
User Interface - Session type	*Output only, Transaction processing, Interactive*	
User Interface - Scope of Utilities	*Limited, Full*	
External environment	*Hostile, Neutral, Benign*	

Table A.2 provides a record of the risk assessment values derived from the system security parameters.

Table A.2 Risk Assessment Record

Risk Assessment Record		
System Identity		
Evaluation level		
User Group Identity		
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	
Most sensitive category type	*0, 1, 2*	
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	
Number of users at minimum clearance	*-0.25, 0, 0.25*	
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	
R_{adj}	*-1, 0, 1*	
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	
Security environment type	*-0.5, 0*	
Terminal type	*0, 1, 2*	
Session type	*0, 1, 2*	
Scope of utilities	*0, 1*	
User interface	*-1, -0.5, 0, 0.5*	
External environment	*-0.5, 0, 0.5*	
R_{sys}	*-2, -1, 0, 1*	
Risk Index	*0, 1, 2, 3, 4*	

A.2 Network Security Tables

Table A.3 provides a record of the network security parameters.

Table A.3 Network Security Parameter Table

Network Security Parameter Table								
Zone ID								
Table Evaluation Level								
Table Minimum								
Table Maximum								
Component ID	***ITSEC Eval. Level***	***ITSEC Func. Class***	***Least Cleared User***	***Processing Range***	***Export Range***	***Import Range***	***Min***	***Max***

Notes

1. The column entitled ***Processing Range*** refers to the range of sensitivity levels over which the component stores and processes data.
2. The column entitled ***Export Range*** refers to the range of sensitivity levels over which the component exports data within the zone.
3. The column entitled ***Import Range*** refers to the range of sensitivity levels over which the component imports data within the zone.
4. The column entitled ***Min*** refers to the minimum of:
   a. the clearance level of the lowest cleared direct user of the component; and
   b. lower bound of the export range.
5. The column entitled ***Max*** refers to the maximum of:
   a. upper bound of the processing range; and
   b. upper bound of the import range.
6. The ***Table Minimum*** refers to the minimum of the component minima.
7. The ***Table Maximum*** refers to the maximum of the component maxima.

Table A.4 provides a record of the inter-zone data flow.

Table A.4 Inter-zone Data Flow Table

Inter-zone Data Flow Table							
Sending Zone			*Receiving Zone*			*Interconnection Device*	
ID	*Eval. Level*	*Processing Range*	*ID*	*Processing Range*	*Least Cleared User*	*Type*	*Eval. Level*

APPENDIX B ALLIES NATIONAL SECURITY EQUIVALENCE TABLES

B.1 Data Classification Levels

Table B.1 provides broad equivalences between the Australian data classification levels and the US and UK counterparts.

Table B.1 Data Classification Equivalences

Data classification equivalences		
Australia	*US*	*UK*
Restricted (R)	Not classified but sensitive (N)†	Restricted (R)
Confidential (C)	Confidential (C)	Confidential (C)
Secret (S)	Secret (S)	Secret (S)
Top Secret (TS)	Top Secret (TS)	Top Secret (TS)

Note
The table does not take into the account the presence of categories since there is no generalised equivalence relationship.

† Also known as For Official Use Only (FOUO).

B.2 User Clearance Levels

Table B.2 provides broad equivalences between the Australian user clearance levels and the US and UK counterparts.

Table B.2 User Clearance Equivalences

User Clearance equivalences		
Australia	*US*	*UK*
Restricted (R)	Not Cleared but Authorised Access to Sensitive Unclassified Information (N)	Not Cleared but known or operating under supervision
Confidential (C)	Confidential (C)	Negative Vetting (NV)
Secret (S)	Secret (S)	Positive Vetting - Secret (S)
Top Secret through Negative Vetting (TS(NV))	Top Secret /Current Background Investigation (TS(BI))	Positive Vetting (PV)
Top Secret through Positive Vetting (TS(PV))	Top Secret /Current Special Background Investigation (TS(SBI))	Enhanced Positive Vetting (EPV)

APPENDIX C MAPPINGS OF ITSEC TO OTHER SECURITY CRITERIA

C.1 Relationship between ITSEC and TCSEC

The TCSEC, established a uniform set of evaluation classes which satisfy specific security requirements. These requirements are grouped according to the security control objectives which are satisfied. These objectives are:

- Security Policy;
- Accountability;
- Assurance; and
- Documentation.

A total of seven classes are identified (D, C1, C2, B1, B2, B3, and A1), grouped in four divisions (D, C, B, and A). Each class satisfies a specific set of security objectives, indicating both security functionality and the level of assurance offered.

Table C.1 provides a correspondence between the ITSEC criteria and the TCSEC classes.

Table C.1 ITSEC/TCSEC Equivalences

ITSEC criteria to TCSEC classes	
ITSEC Criteria	*TCSEC Class*
E0	D
F-C1,E2	C1
F-C2,E2	C2
F-B1,E3	B1
F-B2,E4	B2
F-B3,E5	B3
F-B3,E6	A1

Note
There is no TCSEC class equivalent to the ITSEC evaluation level E1.

C.1.1 Rationale for ITSEC to TCSEC Assurance Criteria Mappings

Table C.1 is taken from para. 1.36 of ITSEC under "Relationship to the TCSEC".

C.2 Relationship between ITSEC and CESG Computer Security Memorandum No 3

The UK GCHQ document defines a standard set of UK Systems Security Confidence Levels. A total of seven confidence levels are identified. Each level is described in terms of the required provisions and approach under the following aspects of the development process:

- specification of security requirements;
- architectural definition;
- implementation;
- evaluation;
- documentation; and
- configuration control.

Security functionality is not addressed in this document.

Table C.2 provides a correspondence between the ITSEC Evaluation levels and the CESG confidence level.

Table C.2 ITSEC/CESG Equivalences

ITSEC Evaluation levels to CESG Confidence levels	
ITSEC Evaluation level	*CESG Confidence level*
E0	UKL0
E1	UKL0
E2	UKL1/UKL2
E3	UKL3
E4	UKL4
E5	UKL5
E6	UKL6

Notes

1. This table indicates which CESG confidence level will be satisfied by a system evaluated to an specific ITSEC level.
2. The converse mapping does not necessarily hold due to the wider confidence requirements found in the ITSEC criteria.
3. ITSEC evaluation level E1 criteria do not fully satisfy the UKL1 criteria (in the area of configuration control).

C.2.1 Rationale for ITSEC to CESG Assurance Criteria Mappings

The following is a list of ITSEC requirements which satisfy, by aspect of the development process, the UK Confidence level requirements:

1. ***UKL0 Unassured***
   No requirements.
2. ***UKL1 Vendor Assured***

   a. Specification of security requirements
      Security Target (E1)
   b. Architectural definition
      No requirements.
   c. Implementation
      No requirements.
   d. Evaluation
      Independent Objectives Testing (E1), *Test Documentation* (E2)
   e. Documentation
      Informal Architectural Design Specification (E1),*Informal External Interface Specification* (E1)
   f. Configuration control
      Configuration Control System (E2)

3. *UKL2 Independently Tested*

   a. Specification of security requirements
      Security Target (E1)
   b. Architectural definition
      Informal Description of Architecture (E1)
   c. Implementation
      Testing against Security Target (E1), *Evidence of Developer Testing* (E2)
   d. Evaluation
      Independent Objectives Testing (E1), *Test Documentation* (E2)
   e. Documentation
      No additional requirements.
   f. Configuration control
      Approved Distribution Procedure (E2), *Audited Sysgen Procedure* (E2)

4. *UKL3 Independently Assured*

   a. Specification of security requirements
      Security Target (E1)
   b. Architectural definition
      Informal Description of Architecture (E1)
   c. Implementation
      No additional requirements.
   d. Evaluation
      < criteria needed >
   e. Documentation
      Informal Description of Detailed Design (E2),*Test Documentation* (E2), *Library of Test Programs* (E2), *Source Code* (E3)
   f. Configuration control
      Acceptance Procedure (E3)

5. *UKL4 Structurally Sound*

   a. Specification of security requirements
      No additional requirements.
   b. Architectural definition
      Structured Description of Architecture (E4)
   c. Implementation
      No additional requirements.
   d. Evaluation
      No equivalent criteria
   e. Documentation
      No additional requirements.
   f. Configuration control
      Acceptance Procedure (E3)

6. *UKL5 Rigorous Design*

   a. Specification of security requirements
      Formal Security Policy Model (E4)
   b. Architectural definition
      Structured Description of Architecture (E4)
   c. Implementation
      Implementation Vulnerability Analysis (E5), *Source Code matches Detailed Design* (E5)
   d. Evaluation
      No equivalent criteria needed
   e. Documentation
      Formal description and associated consistency proofs of key security functions (E4), *Description of design vulnerability analysis and its results* (E4), *Description of the implementation vulnerability analysis and its results* (E5)

f. Configuration control
Configuration Control on all Objects (E5)

7. ***UKL6 Assured Design***

a. Specification of security requirements
No additional requirements.
b. Architectural definition
Formal Description of Architecture (E6)
c. Implementation
Object Code matches Source Code (E6)
d. Evaluation
Approved Languages only (E6)
e. Documentation
Formal Architectural Design Spec (E6), *Description of the methods and tools used to provide the formal proofs of consistency of the model and the architectural specification* (E6)
f. Configuration control
No additional requirements.

APPENDIX D CASE STUDIES

D.1 Sea Surface Surveillance System (S4)

This example is based on the Landwehr and Lubbes example given in the paper "Determining Security Requirements for Complex Systems with the Orange Book" of a hypothetical system which keeps track of objects on the surface of the seas. The system collects information from a variety of open and secret sources and distributes it to a variety of customers. The system maintains a data base of sighting information that is both automatically and manually updated.

The example has been embellished with more environmental detail in order to demonstrate the effects of the various factors on the final TCS recommendation.

The system operates in a Multilevel security mode and processes data up to TS level with a number of compartments. The system data base contains 250 Mbytes of data and 20 Mbytes of this data is classified at the TS level.

There are three main user groups:

1. *System Management Personnel*
   This group is responsible for performing all system and security functions. The group comprises a System Manager, and two Operators. All users in this group are cleared to Top Secret (PV) level. The users have interactive connections via dumb terminals and have access to system utilities.
2. *Analysts*
   This group is responsible for the resolution of ambiguities when the system cannot associate a particular sighting with a particular platform, they can cause messages to be sent to subscribers automatically on a regular basis, and they can update the data base. The group comprises 50 users, all cleared to Top Secret (PV) level. The analysts enter commands via intelligent workstations. Only pre-formatted commands are accepted by the system.
3. *Remote Subscribers*
   This group are recipients of reports generated by the system. They are located remotely via receive-only terminals. The group comprises 110 users, with clearances ranging from Secret to Top Secret (NV) with 10 users cleared to Secret. They cannot directly enter data into the system, but they can issue fixed-format commands to request the location of particular objects.

The operational environment is subject to configuration control mechanisms. However, the operators are permitted to perform application maintenance functions. The system is located in a highly secure military headquarters building.

The risk assessment is carried out in three different ways in order to demonstrate how it is possible to reduce the TCS requirement by applying more sophisticated assessment techniques.

Table D.1 Security Parameters S4 — Limited Yellow Book Assessment

Security Parameters Record		
System Identity	**S4**	
Evaluation level	-	
User Group Identity	**All users**	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**S**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**
Total volume of data	*MBytes*	-
Volume of data at the maximum sensitivity level	*MBytes*	-
Total number of users in the group	*1 to N*	-
Number of users at the minimum clearance level	*1 to N*	-
Security environment type	*Open, Closed*	**Open**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	-
User Interface - Session type	*Output only, Transaction processing, Interactive*	-
User Interface - Scope of Utilities	*Limited, Full*	-
External environment	*Hostile, Neutral, Benign*	-

Table D.2 Risk Assessment S4 — Limited Yellow Book Assessment

Risk Assessment Record		
System Identity	S4	
Evaluation level	-	
User Group Identity	**All Users (limited Yellow Book)**	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	**3**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	-
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	-
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	-
Number of users at minimum clearance	*-0.25, 0, 0.25*	-
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	-
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	-
R_{adj}	*-1, 0, 1*	-
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**4**
Security environment type	*-0.5, 0*	**0**
Terminal type	*0, 1, 2*	-
Session type	*0, 1, 2*	-
Scope of Utilities	*0, 1*	-
User interface	*-1, -0.5, 0, 0.5*	-
External environment	*-0.5, 0, 0.5*	-
R_{sys}	*-2, -1, 0, 1*	**0**
Risk Index	*0, 1, 2, 3, 4*	**4**

The Risk Index indicates a minimum requirement of ***ITSEC evaluation level E6 (TCSEC A1)*** is required.

Table D.3 Security Parameters S4 — Full Assessment with single user group

Security Parameters Record		
System Identity	**S4**	
Evaluation level	-	
User Group Identity	**All users**	
Item Description	*Valid Range*	*Parameter*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**S**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**
Total volume of data	*MBytes*	**250**
Volume of data at the maximum sensitivity level	*MBytes*	**20**
Total number of users in the group	*1 to N*	**163**
Number of users at the minimum clearance level	*1 to N*	**10**
Security environment type	*Open, Closed*	**Open**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	**Full function - intelligent**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**
User Interface - User expertise	*Limited, Full*	**Full**
External environment	*Hostile, Neutral, Benign*	**Benign**

Table D.4 Risk Assessment S4 — Full Assessment with single user group

Risk Assessment Record		
System Identity	S4	
Evaluation level	-	
User Group Identity	**All Users (full)**	
Item Description	*Valid Values*	*Value*
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**3**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**-0.25**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**-0.25**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**-0.5**
R_{adj}	*-1, 0, 1*	**-1**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**3**
Security environment type	*-0.5, 0*	**0**
Terminal type	*0, 1, 2*	**2**
Session type	*0, 1, 2*	**2**
Scope of Utilities	*0, 1*	**1**
User interface	*-1, -0.5, 0, 0.5*	**0.5**
External environment	*-0.5, 0, 0.5*	**-0.5**
R_{sys}	*-2, -1, 0, 1*	**0**
Risk Index	*0, 1, 2, 3, 4*	**3**

The Risk Index of 3 indicates a minimum requirement of ***ITSEC evaluation level E5 (TCSEC B3)*** is required.

Table D.5 Security Parameters S4 — Full Assessment with multiple user groups

Security Parameters Record				
System Identity	S4			
Evaluation level	-			
User Group Identity	G1 (System Management), G2 (Analysis), G3 (Subscribers)			
Item Description	*Valid Range*	*G1 Parameter*	*G2 Parameter*	*G3 Parameter*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**	**TS**	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**TS(PV)**	**TS(PV)**	**S**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**	**Compartment**	**Compartment**
Total volume of data	*MBytes*	**250**	**250**	**250**
Volume of data at the maximum sensitivity level	*MBytes*	**20**	**20**	**20**
Total number of users in the group	*1 to N*	**3**	**50**	**110**
Number of users at the minimum clearance level	*1 to N*	**3**	**50**	**10**
Security environment type	*Open, Closed*	**Open**	**Open**	**Open**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	**Full function - dumb**	**Full function - intelligent**	**Limited function**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**	**Transaction processing**	**Transaction processing**
User Interface - Scope of Utilities	*Limited, Full*	**Full**	**Limited**	**Limited**
External environment	*Hostile, Neutral, Benign*	**Benign**	**Benign**	**Benign**

Table D.6 Risk Assessment S4 — Full Assessment with multiple user groups

Risk Assessment Record				
System Identity	S4			
Evaluation level	•			
User Group Identity	G1 (System Management), G2 (Analysts), G3 (Subscribers)			
Item Description	***Valid Values***	***G1***	***G2***	***G3***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	5	5	5
Most sensitive category type	*0, 1, 2*	2	2	2
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	7	7	7
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	7	7	3
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	0	0	0
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	0	0	0
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	0	0	0
Number of users at minimum clearance	*-0.25, 0, 0.25*	0	0	-0.25
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	0	0	-0.25
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	0	0	-0.5
R_{adj}	*-1, 0, 1*	0	0	-1
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	0	0	3
Security environment type	*-0.5, 0*	0	0	0
Terminal type	*0, 1, 2*	1	2	0
Session type	*0, 1, 2*	2	1	1
Scope of Utilities	*0, 1*	1	0	0
User interface	*-1, -0.5, 0, 0.5*	0	0	-0.5
External environment	*-0.5, 0, 0.5*	-0.5	-0.5	-0.5
R_{sys}	*-2, -1, 0, 1*	-1	-1	-1
Risk Index	*0, 1, 2, 3, 4*	0	0	2

Taking the worst case Risk Index of 2, a minimum requirement of ***ITSEC evaluation level E5 (TCSEC B2)*** is required

D.2 Command Support System (CSS)

This example is an information handling system supporting a number of applications which facilitate the strategic decision making process of the military high command and, additionally, carry out administrative support functions.

The system comprises a network of workstations and supports a relational data base which is accessed through an SQL server application. The majority of users interface with the system via a menu-based user interface application. No software development tools are available on this system, software development being done on a separate development system. All new or updated applications are manually verified and loaded by a system programmer and are subject to strict configuration control procedures.

The application developers are not authorised to have access to the production system and there are sufficient physical protection measures to preclude the developers from having physical access to the terminals connected to the production system.

There is a total of 1500 Mbytes of data on the system and the classification levels are distributed as follows:

> 1350 Mbytes at Confidential or below;
>
> 100 Mbytes at Secret; and
>
> 50 Mbytes at Top Secret (including 15 Mbytes of compartmented data).

The users of the system may be categorised as follows:

1. ***System Management***
   This group is responsible for maintenance and operation of the network including the security functions. The group comprises 5 members: a Network Manager, Database Manager, Security Officer, and two System Programmers. The system programmers perform the loading of all new software and all other operational functions. These users are all cleared to TS(PV). This group has access to the operating system commands.
2. ***Operations***
   This group is responsible for the operational aspects of the system. All users are cleared to TS(NV) level but have no authorisation to access compartmented data. There are 20 users in this group. The interface to the system is via the transaction processing application.
3. ***Special Operations***
   This group is responsible for the more sensitive operational aspects of the system. There are 5 users in the group all of which are cleared to TS(PV) level and possess authorisations to access some compartmented data. The interface to the system is via the transaction processing application.
4. ***Administrative Support***
   This group is responsible for the personnel, accounting, and other administrative functions. There are 70 users who are cleared to Secret level. The interface to the system is via the transaction processing application.

The system is located in a defence headquarters building which is subject to stringent physical security measures.

The risk assessment is carried out using the Limited Yellow Book and the multiple user groups approach.

Table D.7 Security Parameters CSS — Limited Yellow Book Assessment

Security Parameters Record		
System Identity	CSS	
Evaluation level	-	
User Group Identity	**All users**	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**S**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**
Total volume of data	*MBytes*	-
Volume of data at the maximum sensitivity level	*MBytes*	-
Total number of users in the group	*1 to N*	-
Number of users at the minimum clearance level	*1 to N*	-
Security environment type	*Open, Closed*	**Closed**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	-
User Interface - Session type	*Output only, Transaction processing, Interactive*	-
User Interface - Scope of Utilities	*Limited, Full*	-
External environment	*Hostile, Neutral, Benign*	-

Table D.8 Risk Assessment CSS — Limited Yellow Book Assessment

Risk Assessment Record		
System Identity	**CSS**	
Evaluation level	**-**	
User Group Identity	**All Users (limited Yellow Book)**	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**3**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**-**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**-**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**-**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**-**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**-**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**-**
R_{adj}	*-1, 0, 1*	**-**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**4**
Security environment type	*-0.5, 0*	**-0.5**
Terminal type	*0, 1, 2*	**-**
Session type	*0, 1, 2*	**-**
Scope of Utilities	*0, 1*	**-**
User interface	*-1, -0.5, 0, 0.5*	**-**
External environment	*-0.5, 0, 0.5*	**-**
R_{sys}	*-2, -1, 0, 1*	**-1**
Risk Index	*0, 1, 2, 3, 4*	**3**

The Risk Index indicates a minimum requirement of ***ITSEC evaluation level E5 (TCSEC B3)*** is required.

Table D.9 Security Parameters CSS — Full Assessment with single User Group

Security Parameters Record		
System Identity	CSS	
Evaluation level	-	
User Group Identity	**All users**	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**S**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**
Total volume of data	*MBytes*	**1500**
Volume of data at the maximum sensitivity level	*MBytes*	**50**
Total number of users in the group	*1 to N*	**100**
Number of users at the minimum clearance level	*1 to N*	**70**
Security environment type	*Open, Closed*	**Closed**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	**Full function - intelligent**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**
User Interface - User expertise	*Limited, Full*	**Full**
External environment	*Hostile, Neutral, Benign*	**Benign**

Table D.10 Risk Assessment CSS — Full Assessment with single User Group

Risk Assessment Record		
System Identity	CSS	
Evaluation level	-	
User Group Identity	All Users (full)	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	**3**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**0**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**0**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**
R_{adj}	*-1, 0, 1*	**0**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**4**
Security environment type	*-0.5, 0*	**-0.5**
Terminal type	*0, 1, 2*	**2**
Session type	*0, 1, 2*	**2**
Scope of Utilities	*0, 1*	**1**
User interface	*-1, -0.5, 0, 0.5*	**0.5**
External environment	*-0.5, 0, 0.5*	**-0.5**
R_{sys}	*-2, -1, 0, 1*	**-1**
Risk Index	*0, 1, 2, 3, 4*	**3**

The Risk Index indicates a minimum requirement of ***ITSEC evaluation level E5 (TCSEC B3)*** is required.

Table D.11 Security Parameters CSS — Full Assessment with multiple User Groups

Security Parameters Record					
System Identity	CSS				
Evaluation level	-				
User Group Identity	G1 (System Management), G2 (Operations), G3 (Special Operations), G4 (Admin Support)				
Item Description	*Valid Range*	*G1 Parameter*	*G2 Parameter*	*G3 Parameter*	*G4 Parameter*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	TS	TS	TS	TS
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	TS(PV)	TS(NV)	TS(PV)	S
Most sensitive category type	*Caveat, Compartment, None*	Compartment	Compartment	Compartment	Compartment
Total volume of data	*MBytes*	1500	1500	1500	1500
Volume of data at the maximum sensitivity level	*MBytes*	50	50	50	50
Total number of users in the group	*1 to N*	5	20	5	70
Number of users at the minimum clearance level	*1 to N*	5	20	5	70
Security environment type	*Open, Closed*	Closed	Closed	Closed	Closed
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	Full function - intelligent	Full function - intelligent	Full function - intelligent	Full function - intelligent
User Interface - Session type	*Output only, Transaction processing, Interactive*	Interactive	Transaction processing	Transaction processing	Transaction processing
User Interface - Scope of Utilities	*Limited, Full*	Full	Limited	Limited	Limited
External environment	*Hostile, Neutral, Benign*	Benign	Benign	Benign	Benign

Table D.12 Risk Assessment CSS — Full Assessment with multiple User Groups

Risk Assessment Record					
System Identity	CSS				
Evaluation level	-				
User Group Identity	G1 (System Management), G2 (Operations), G3 (Special Operations), G4 (Admin Support)				
Item Description	*Valid Values*	*G1*	*G2*	*G3*	*G4*
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	5	5	5	5
Most sensitive category type	*0, 1, 2*	2	2	2	2
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	7	7	7	7
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	7	5	7	3
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	0	0	0	0
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	0	0	0	0
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	0	0	0	0
Number of users at minimum clearance	*-0.25, 0, 0.25*	0	0	0	0
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	0	0	0	0
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	0	0	0	0
R_{adj}	*-1, 0, 1*	0	0	0	0
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	0	2	0	4
Security environment type	*-0.5, 0*	-0.5	-0.5	-0.5	-0.5
Terminal type	*0, 1, 2*	2	2	2	2
Session type	*0, 1, 2*	2	1	1	1
Scope of Utilities	*0, 1*	1	0	0	0
User interface	*-1, -0.5, 0, 0.5*	0.5	0	0	0
External environment	*-0.5, 0, 0.5*	-0.5	-0.5	-0.5	-0.5
R_{sys}	*-2, -1, 0, 1*	-1	-1	-1	-1
Risk Index	*0, 1, 2, 3, 4*	0	1	0	3

Taking the worst case Risk Index of 3, a minimum requirement of ***ITSEC evaluation level E5 (TCSEC B3)*** is required, which is the same as the Yellow Book assessment.

D.3 Civilian System (DEPT X)

This example is of a hypothetical government department system.

The system holds a small number of sensitive files classified as Protected. The vast majority of the files stored and processed on the system are either In-Confidence or Unclassified. The files classified as Protected are imported from another system, having undergone a manual review to ensure the correctness of the security labels prior to release from the originator, and are not updated on this system.

The system holds a total of 400 Mbytes of data of which only 2 Mbytes is classified as Protected. The system runs a dedicated Office Automation package and all users with the exception System

Administrators and Operators communicate with the system exclusively through this package. All users access the system via PCs. Only the System Administrators and Operators have direct access to operating system commands.

There are four main user groups:

1. *System Administration*
   This group is responsible for running the system including the security aspects. The group comprises a DP Manager (who is the security officer), a Systems Programmer, and Database Administrator. These users are all cleared to access Protected material. This group has unlimited access to the system utilities.
2. *Operators*
   This group comprises 4 operators who are all cleared to access Protected material. The operators have direct access to a limited set of utilities to perform backups and control printing.
3. *Data Entry*
   This group is responsible for entry and modification of unclassified and In-Confidence records. The group comprises 100 users, 80 of which have authorisation to process In-Confidence records.
4. *Executive Officers*
   This group is responsible for the departmental policy decisions based on information stored on the system. The group comprises 10 users who are cleared to access all data on the system.

The operational environment is subject to configuration control mechanisms, however, the applications running on the system were developed by uncleared personnel. The system is located in a city centre office.

The risk assessment is carried out firstly taking all users together, and then by separating out the user groups.

Table D.13 Security Parameters DEPT X — Full Assessment with single User Group

Security Parameters Record		
System Identity	**DEPT X**	
Evaluation level	-	
User Group Identity	**All users**	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**P**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**U**
Most sensitive category type	*Caveat, Compartment, None*	**None**
Total volume of data	*MBytes*	**400**
Volume of data at the maximum sensitivity level	*MBytes*	**2**
Total number of users in the group	*1 to N*	**117**
Number of users at the minimum clearance level	*1 to N*	**20**
Security environment type	*Open, Closed*	**Open**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	**Full function - intelligent**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**
User Interface - Scope of Utilities	*Limited, Full*	**Full**
External environment	*Hostile, Neutral, Benign*	**Neutral**

Table D.14 Risk Assessment DEPT X — Full Assessment with single User Group

Risk Assessment Record		
System Identity	**DEPT X**	
Evaluation level	-	
User Group Identity	**All Users**	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**2**
Most sensitive category type	*0, 1, 2*	**0**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**2**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**0**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**-0.25**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**-0.25**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**-0.5**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**0**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**0**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**
R_{adj}	*-1, 0, 1*	**-1**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**1**
Security environment type	*-0.5, 0*	**0**
Terminal type	*0, 1, 2*	**2**
Session type	*0, 1, 2*	**2**
Scope of Utilities	*0, 1*	**1**
User interface	*-1, -0.5, 0, 0.5*	**0.5**
External environment	*-0.5, 0, 0.5*	**0**
R_{sys}	*-2, -1, 0, 1*	**0**
Risk Index	*0, 1, 2, 3, 4*	**1**

The Risk Index of 1 indicates a minimum requirement of *ITSEC evaluation level E3 (TCSEC B1)* is required.

Table D.15 Security Parameters DEPT X — Full Assessment with multiple User Groups

Security Parameters Record					
System Identity	DEPT X				
Evaluation level	-				
User Group Identity	G1 (System Admin), G2 (Operators), G3 (Data Entry), G4 (Execs)				
Item Description	*Valid Range*	*G1*	*G2*	*G3*	*G4*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**P**	**P**	**P**	**P**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**P**	**P**	**U**	**P**
Most sensitive category type	*Caveat, Compartment, None*	**None**	**None**	**None**	**None**
Total volume of data	*MBytes*	**400**	**400**	**400**	**400**
Volume of data at the maximum sensitivity level	*MBytes*	**2**	**2**	**2**	**2**
Total number of users in the group	*1 to N*	**3**	**4**	**100**	**10**
Number of users at the minimum clearance level	*1 to N*	**3**	**4**	**20**	**10**
Security environment type	*Open, Closed*	**Open**	**Open**	**Open**	**Open**
User Interface - Terminal type	*Limited function, Full Function - dumb, Full function - intelligent*	**Full function - int**	**Full function - dumb**	**Full function - dumb**	**Full function - int**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**	**Interactive**	**Trans proc**	**Trans proc**
User Interface - Scope of Utilities	*Limited, Full*	**Full**	**Limited**	**Limited**	**Limited**
External environment	*Hostile, Neutral, Benign*	**Neutral**	**Neutral**	**Neutral**	**Neutral**

Table D.16 Risk Assessment DEPT X — Full Assessment with multiple User Groups

Risk Assessment Record					
System Identity	**DEPT X**				
Evaluation level	-				
User Group Identity	**G1 (Admin), G2 (Operators), G3 (Data Entry), G4 (Exec)**				
Item Description	***Valid Values***	***G1***	***G2***	***G3***	***G4***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**2**	**2**	**2**	**2**
Most sensitive category type	*0, 1, 2*	**0**	**0**	**0**	**0**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**2**	**2**	**2**	**2**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**2**	**2**	**0**	**2**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**-0.25**	**0**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**-0.25**	**0**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**-0.5**	**0**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**0**	**0**
R_{adj}	*-1, 0, 1*	**0**	**0**	**-1**	**0**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**0**	**0**	**1**	**0**
Security environment type	*-0.5, 0*	**0**	**0**	**0**	**0**
Terminal type	*0, 1, 2*	**2**	**2**	**2**	**2**
Session type	*0, 1, 2*	**2**	**2**	**1**	**1**
Scope of Utilities	*0, 1*	**1**	**0**	**0**	**0**
User interface	*-1, -0.5, 0, 0.5*	**0.5**	**0**	**0**	**0**
External environment	*-0.5, 0, 0.5*	**0**	**0**	**0**	**0**
R_{sys}	*-2, -1, 0, 1*	**0**	**0**	**0**	**0**
Risk Index	*0, 1, 2, 3, 4*	**0**	**0**	**1**	**0**

The worst case Risk Index of 1 indicates a minimum requirement of ***ITSEC evaluation level E3 (TCSEC B1)*** is required. In this case, the separation into user groups did not produce a reduction in risk.

Table D.17 Security Parameters DEPT X — Full Assessment with multiple User Groups

Security Parameters Record					
System Identity	DEPT X				
Evaluation level	-				
User Group Identity	G1 (System Admin), G2 (Operators), G3 (Data Entry), G4 (Execs)				
Item Description	*Valid Range*	*G1*	*G2*	*G3*	*G4*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**P**	**P**	**P**	**P**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**P**	**P**	**U**	**P**
Most sensitive category type	*Caveat, Compartment, None*	**None**	**None**	**None**	**None**
Total volume of data	*MBytes*	**400**	**400**	**400**	**400**
Volume of data at the maximum sensitivity level	*MBytes*	**2**	**2**	**2**	**2**
Total number of users in the group	*1 to N*	**3**	**4**	**100**	**10**
Number of users at the minimum clearance level	*1 to N*	**3**	**4**	**20**	**10**
Security environment type	*Open, Closed*	**Open**	**Open**	**Open**	**Open**
User Interface - Terminal type	*Limited function, Full Function - dumb, Full function - intelligent*	**Full function - int**	**Full function - dumb**	**Full function - dumb**	**Full function - int**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Interactive**	**Interactive**	**Trans proc**	**Trans proc**
User Interface - Scope of Utilities	*Limited, Full*	**Full**	**Limited**	**Limited**	**Limited**
External environment	*Hostile, Neutral, Benign*	**Neutral**	**Neutral**	**Neutral**	**Neutral**

Table D.18 Risk Assessment DEPT X — Full Assessment with multiple User Groups

Risk Assessment Record					
System Identity	**DEPT X**				
Evaluation level	**-**				
User Group Identity	**G1 (Admin), G2 (Operators), G3 (Data Entry), G4 (Exec)**				
Item Description	***Valid Values***	***G1***	***G2***	***G3***	***G4***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**2**	**2**	**2**	**2**
Most sensitive category type	*0, 1, 2*	**0**	**0**	**0**	**0**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**2**	**2**	**2**	**2**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**2**	**2**	**0**	**2**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**-0.25**	**0**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**-0.25**	**0**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**-0.5**	**0**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**0**	**0**
R_{adj}	*-1, 0, 1*	**0**	**0**	**-1**	**0**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**0**	**0**	**1**	**0**
Security environment type	*-0.5, 0*	**0**	**0**	**0**	**0**
Terminal type	*0, 1, 2*	**2**	**2**	**2**	**2**
Session type	*0, 1, 2*	**2**	**2**	**1**	**1**
Scope of Utilities	*0, 1*	**1**	**0**	**0**	**0**
User interface	*-1, -0.5, 0, 0.5*	**0.5**	**0**	**0**	**0**
External environment	*-0.5, 0, 0.5*	**0**	**0**	**0**	**0**
R_{sys}	*-2, -1, 0, 1*	**0**	**0**	**0**	**0**
Risk Index	*0, 1, 2, 3, 4*	**0**	**0**	**1**	**0**

The worst case Risk Index of 1 indicates a minimum requirement of ***ITSEC evaluation level E3 (TCSEC B1)*** is required. In this case, the separation into user groups did not produce a reduction in risk.

D.4 Compartmented System (COMP)

This example describes a system operating in Compartmented mode under which the Yellow Book "minimum" TCS requirement can be reduced if system factors are taken into account.

The hypothetical system is an intelligence gathering facility processing highly sensitive compartmented material, located in a highly secure central agency office.

The database consists of 100 Mbytes of data, 10 Mbytes is at TS level.

Of the 100 users, 20 are cleared to TS(PV) and the remainder to TS(NV). Not all the users have been authorised access to every compartment. All users are connected to the system via dumb terminals and access the database is via a transaction-based application.

The system is subject to strict configuration control procedures and no software development is carried out on the system. The application software was developed externally by personnel cleared to Secret level.

The risk assessment is done in two ways, the Limited Yellow Book, and the full assessment. In this example, the partitioning into separate user groups is not appropriate since there are no distinctly identifiable subgroups.

Table D.19 Security Parameters COMP — Limited Yellow Book Assessment

Security Parameters Record		
System Identity	COMP	
Evaluation level	-	
User Group Identity	All users	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	TS
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	TS(NV)
Most sensitive category type	*Caveat, Compartment, None*	Compartment
Total volume of data	*MBytes*	-
Volume of data at the maximum sensitivity level	*MBytes*	-
Total number of users in the group	*1 to N*	-
Number of users at the minimum clearance level	*1 to N*	-
Security environment type	*Open, Closed*	Closed
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	-
User Interface - Session type	*Output only, Transaction processing,, Interactive*	-
User Interface - Scope of Utilities	*Limited, Full*	-
External environment	*Hostile, Neutral, Benign*	-

Table D.20 Risk Assessment COMP — Limited Yellow Book Assessment

Risk Assessment Record		
System Identity	COMP	
Evaluation level	-	
User Group Identity	**All Users (limited Yellow Book)**	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users, R_{min}	*0, 1, 2, 3, 5, 7*	**5**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	-
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	-
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	-
Number of users at minimum clearance	*-0.25, 0, 0.25*	-
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	-
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	-
R_{adj}	*-1, 0, 1*	-
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**2**
Security environment type	*-0.5, 0*	**-0.5**
Terminal type	*0, 1, 2*	-
Session type	*0, 1, 2*	-
Scope of Utilities	*0, 1*	-
User interface	*-1, -0.5, 0, 0.5*	-
External environment	*-0.5, 0, 0.5*	-
R_{sys}	*-2, -1, 0, 1*	**-1**
Risk Index	*0, 1, 2, 3, 4*	**2**

The Risk Index indicates a minimum requirement of ***ITSEC evaluation level E4 (TCSEC B2)*** is required.

Table D.21 Security Parameters COMP — Full Assessment with single User Group

Security Parameters Record		
System Identity	**COMP**	
Evaluation level	•	
User Group Identity	**All users**	
Item Description	***Valid Range***	***Parameter***
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	**TS**
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	**TS(NV)**
Most sensitive category type	*Caveat, Compartment, None*	**Compartment**
Total volume of data	*MBytes*	**100**
Volume of data at the maximum sensitivity level	*MBytes*	**10**
Total number of users in the group	*1 to N*	**100**
Number of users at the minimum clearance level	*1 to N*	**80**
Security environment type	*Open, Closed*	**Closed**
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	**Full function - dumb**
User Interface - Session type	*Output only, Transaction processing, Interactive*	**Transaction processing**
User Interface - Scope of Utilities	*Limited, Full*	**Limited**
External environment	*Hostile, Neutral, Benign*	**Benign**

Table D.22 Risk Assessment COMP — Full Assessment with single User Group

Risk Assessment Record		
System Identity	**COMP**	
Evaluation level	-	
User Group Identity	**All Users (full)**	
Item Description	***Valid Values***	***Value***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**5**
Most sensitive category type	*0, 1, 2*	**2**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**7**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**5**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	-
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	-
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	-
Number of users at minimum clearance	*-0.25, 0, 0.25*	-
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	-
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	-
R_{adj}	*-1, 0, 1*	**0**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**2**
Security environment type	*-0.5, 0*	**-0.5**
Terminal type	*0, 1, 2*	**1**
Session type	*0, 1, 2*	**1**
Scope of Utilities	*0, 1*	**0**
User interface	*-1, -0.5, 0, 0.5*	**-0.5**
External environment	*-0.5, 0, 0.5*	**-0.5**
R_{sys}	*-2, -1, 0, 1*	**-1.5**
Risk Index	*0, 1, 2, 3, 4*	**1**

The Risk Index indicates a minimum requirement of ***ITSEC evaluation level E3 (TCSEC B1)*** is required.

D.5 A Network of IAS Components (NET)

The following example is based on a simple network architecture comprising 6 components. The data flow between components is illustrated in Figure D.1.

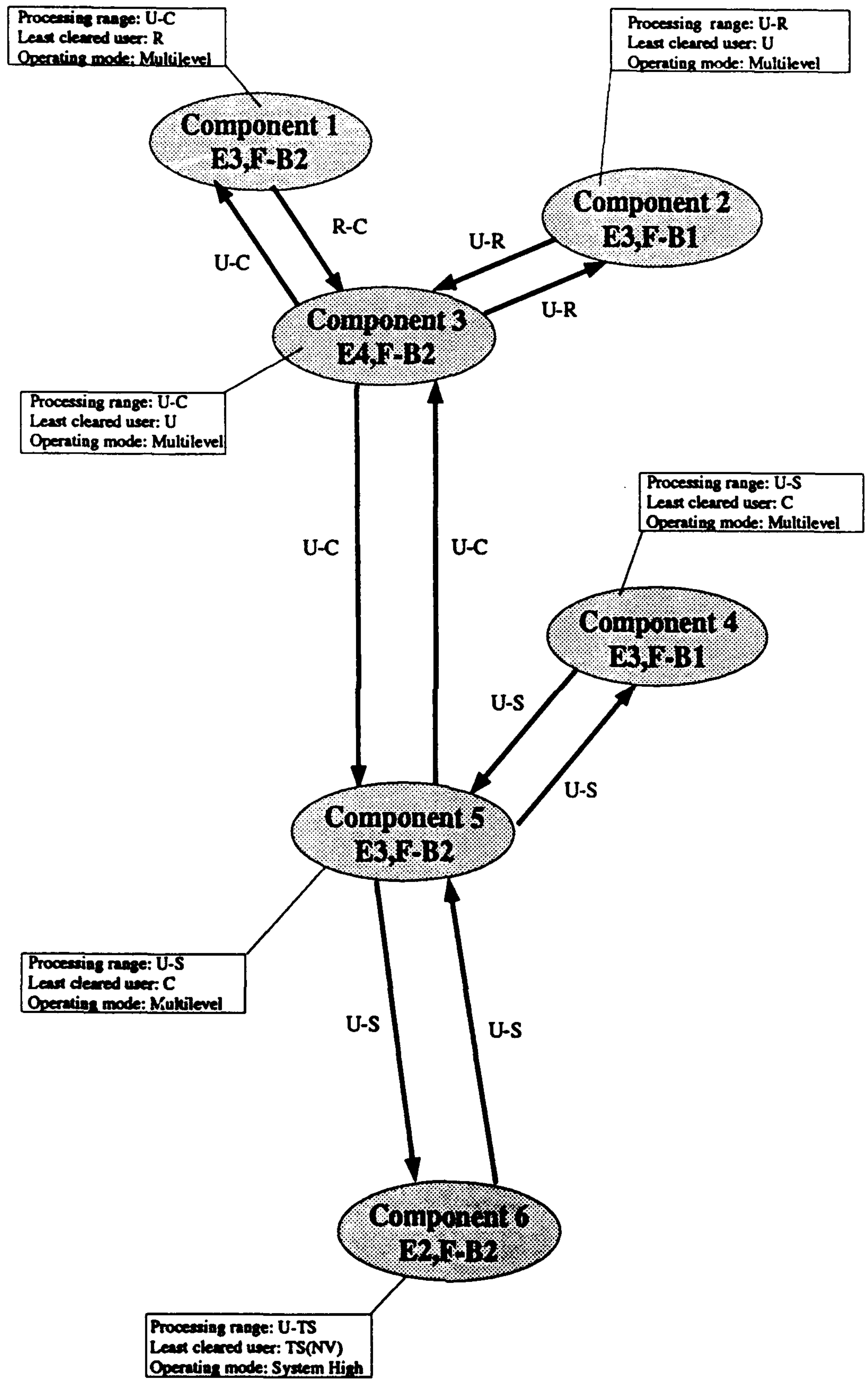


Figure D.1 Network Dataflow

The security parameters for each of the network components are specified in Table D.21.

Table D.23 Security Parameters NET Example

Security Parameters Record							
System Identity	NET						
Evaluation level	-						
User Group Identity	-						
Item Description	*Valid Range*	*Cpt 1*	*Cpt 2*	*Cpt 3*	*Cpt 4*	*Cpt 5*	*Cpt 6*
Maximum Sensitivity of data on the system	*U, R, IC, C, P, S, HP, TS*	C	R	C	S	S	TS
Minimum Clearance of users in the group	*U, R, IC, C, P, S, HP, TS(NV), TS(PV)*	R	U	U	C	C	TS(NV)
Most sensitive category type	*Caveat, Compartment, None*	None	None	None	None	None	None
Total volume of data	*MBytes*	20	10	100	20	20	10
Volume of data at the maximum sensitivity level	*MBytes*	8	5	20	5	5	1
Total number of users in the group	*1 to N*	5	2	10	5	5	2
Number of users at the minimum clearance level	*1 to N*	5	1	1	2	2	2
Security environment type	*Open, Closed*	Open					
User Interface - Terminal type	*Limited function, Full function - dumb, Full function - intelligent*	Full function - intelligent					
User Interface - Session type	*Output only, Transaction processing,, Interactive*	Transaction Processing					
User Interface - Scope of Utilities	*Limited, Full*	Limited					
External environment	*Hostile, Neutral, Benign*	Neutral					

An initial risk assessment of each component in isolation is illustrated in Table D.22.

Table D.24 Risk Assessment NET Example

Risk Assessment Record							
System Identity	NET						
Evaluation level							
User Group Identity	-						
Item Description	***Valid Values***	***Cpt 1***	***Cpt 2***	***Cpt 3***	***Cpt 4***	***Cpt 5***	***Cpt 6***
Maximum Sensitivity of data	*0, 1, 2, 3, 5*	**2**	**1**	**2**	**3**	**3**	**5**
Most sensitive category type	*0, 1, 2*	**0**	**0**	**0**	**0**	**0**	**0**
R_{max}	*0, 1, 2, 3, 4, 5, 6, 7*	**2**	**1**	**2**	**3**	**3**	**5**
Minimum Clearance of users - R_{min}	*0, 1, 2, 3, 5, 7*	**1**	**0**	**0**	**2**	**2**	**5**
Volume of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**	**0**	**0**
Proportion of data at maximum sensitivity	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**	**0**	**0**
A_{data}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**0**	**0**	**0**	**0**
Number of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**	**0**	**0**
Proportion of users at minimum clearance	*-0.25, 0, 0.25*	**0**	**0**	**0**	**0**	**0**	**0**
A_{user}	*-0.5, -0.25, 0, 0.25, 0.5*	**0**	**0**	**0**	**0**	**0**	**0**
R_{adj}	*-1, 0, 1*	**0**	**0**	**0**	**0**	**0**	**0**
DERI	*0, 1, 2, 3, 4, 5, 6, 7, 8*	**1**	**1**	**2**	**1**	**1**	**0**
Security environment type	*-0.5, 0*	**0**	**0**	**0**	**0**	**0**	**0**
Terminal type	*0, 1, 2*	**2**	**2**	**2**	**2**	**2**	**2**
Session type	*0, 1, 2*	**1**	**1**	**1**	**1**	**1**	**1**
Scope of Utilities	*0, 1*	**0**	**0**	**0**	**0**	**0**	**0**
User interface	*-1, -0.5, 0, 0.5*	**0**	**0**	**0**	**0**	**0**	**0**
External environment	*-0.5, 0, 0.5*	**0**	**0**	**0**	**0**	**0**	**0**
R_{sys}	*-2, -1, 0, 1*	**0**	**0**	**0**	**0**	**0**	**0**
Risk Index	*0, 1, 2, 3, 4*	**1**	**1**	**2**	**1**	**1**	**0**

The results of the risk assessment are given in Table D.23.

Table D.25 Minimum Component Evaluation Levels NET Example

Component ID	*Component Evaluation Level*	*Risk Index*	*Minimum Evaluation Level recommended by Guidelines*
1	E3	1	E3
2	E3	1	E3
3	E4	2	E4
4	E3	1	E3
5	E3	1	E3
6	E2	0	E2

Table D.23 indicates that all the components satisfy the recommendations of the Guidelines in isolation.

However, Table D.24 indicates that several of the components do not satisfy the Intra-zone connection rules and the required overall Network Evaluation Level is not achievable, given current COMPUSEC technology.

Table D.26 Network Security Parameter Table NET Example

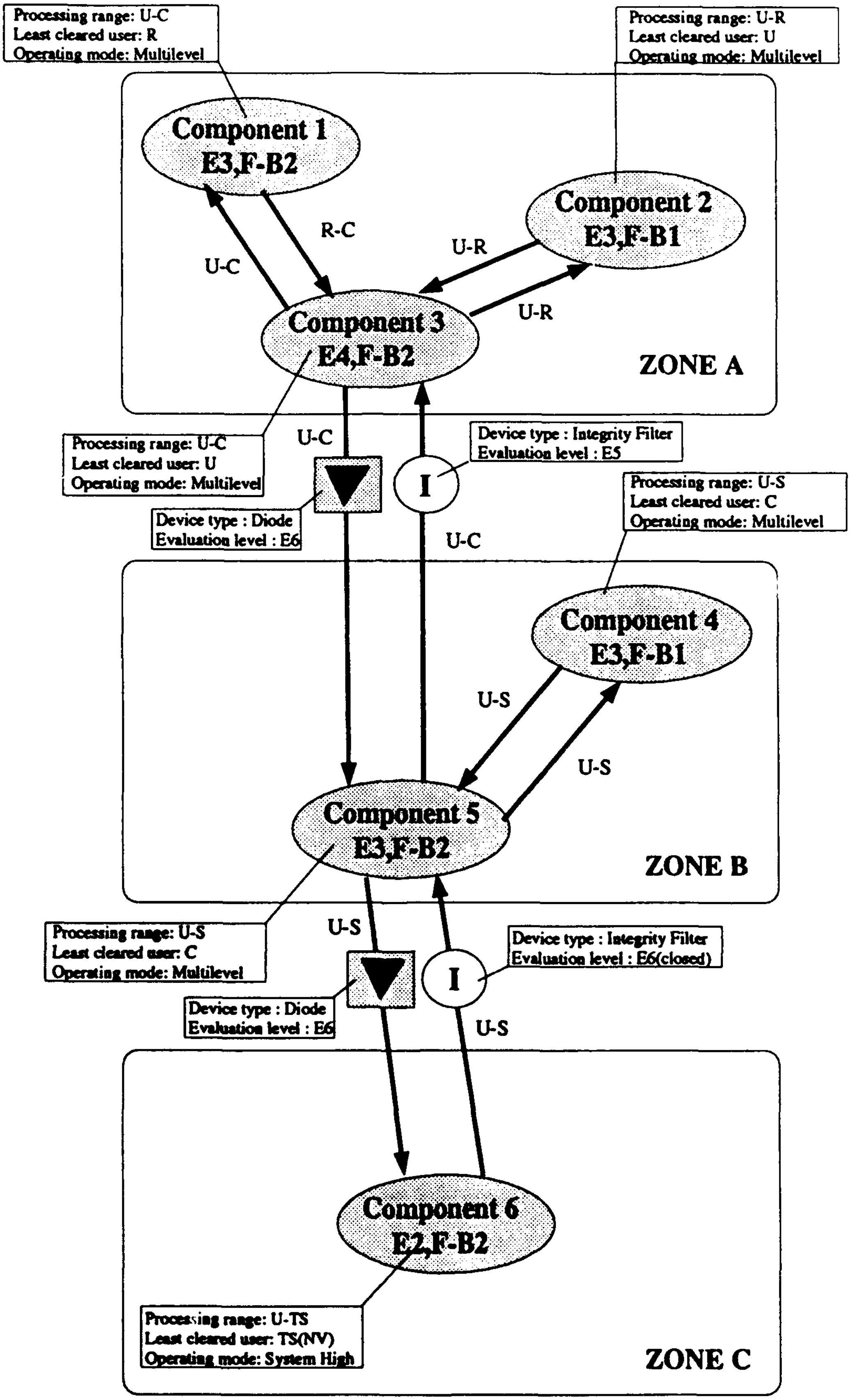
Network Security Parameter Table								
Zone ID				**Whole Network**				
Table Evaluation Level				**see note a.**				
Table Minimum				**U**				
Table Maximum				**TS**				
Component ID	*ITSEC Eval. Level*	*ITSEC Func. Class*	*Least Cleared User*	*Processing Range*	*Export Range*	*Import Range*	*Min*	*Max*
1	E3	F-B2	R	U-C	R-C	U-C	R	C
2	E3	F-B1	U	U-R	U-R	U-R	U	R
3	E4	F-B2	U	U-C	U-C	U-C	U	C
4	E3	F-B1	C	U-S	U-S*	U-S	U	S
5	E3	F-B2	C	U-S	U-S*	U-S	U	S
6	E3	F-B2	TS(NV)	U-TS	U-S*	U-S	U	TS

Notes

1. The evaluation level required to counter this level of risk is beyond the state of current COMPUSEC technology.
2. (*) This range is not allowed by the Intra-zone connection rules.

In order to satisfy the Guidelines it is necessary to partition the network into a number of zones. The partitioned network is represented in Figure D.2.

Figure D.2 Network Dataflow with Zones



For Zone A, the Intra-zone connection rules and Cascading Problem Heuristic are reproduced in Tables D.27 and D.28.

Table D.27 Intra-zone connection test — Zone A

Network Security Parameter Table								
Zone ID				**Zone A**				
Table Evaluation Level				**E4**				
Table Minimum				**U**				
Table Maximum				**C**				
Component ID	***ITSEC Eval. Level***	***ITSEC Func. Class***	***Least Cleared User***	***Processing Range***	***Export Range***	***Import Range***	***Min***	***Max***
1	E3	F-B2	R	U-C	R-C	U-C	R	C
2	E3	F-B1	U	U-R	U-R	U-R	U	R
3	E4	F-B2	U	U-C	U-C	U-C	U	C

Notes

1. The Intra-zone connection rules are satisfied.
2. The Cascading Problem Heuristic must be applied since the Table Evaluation Level is greater than E3.

Table D.28 Cascade Heuristic — Zone A

Network Security Parameter Table								
Zone ID				**Zone A (E3 sub-zone)**				
Table Evaluation Level				**E3***				
Table Minimum				**U**				
Table Maximum				**C**				
Component ID	***ITSEC Eval. Level***	***ITSEC Func. Class***	***Least Cleared User***	***Processing Range***	***Export Range***	***Import Range***	***Min***	***Max***
1	E3	F-B2	R	U-C	R-C	U-C	R	C
2	E3	F-B1	U	U-R	U-R	U-R	U	R

Note
(*) This evaluation level does not satisfy the Guidelines which suggests there is a potential Cascading Path between Component 1 and Component 2.

Although Zone A satisfies the Intra-zone connection rules, there is a potential Cascading Path between Component 1 and Component 2. A possible solution to this problem is to isolate Component 2 in its own zone. Figure D.3 shows a revised architecture for Zone A.

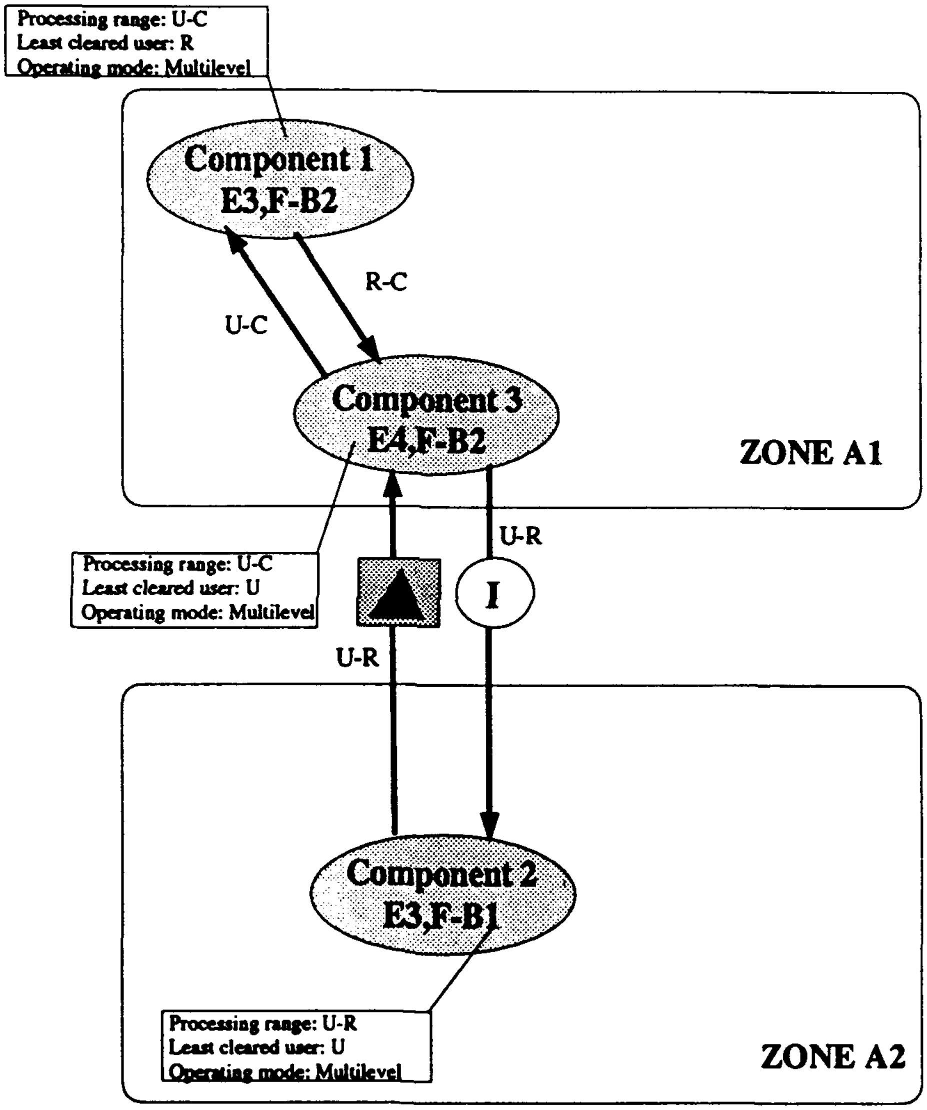


Figure D.3 Zone A Partition

However, for the purposes of this example, we shall ignore this potential cascading path.

For Zone B, which is homogeneous, the components have a common processing range (U-S). Hence, the intra-zone rules and Cascade Heuristic do not apply.

For Zone C, there are no intra-zone connections.

Table D.29 indicates that none of the zones have significant aggregate ancillary factors.

Table D.29 Minimum Zone Evaluation Levels NET Example

Zone ID	*Volume of data at highest classification level*	*Number of Users at lowest clearance level*	*Volume of data Category*	*Number of users Category*
A	130	26	Medium	Medium
B	40	10	Medium	Medium
C	5	1	Low	Low

Finally, we test whether the Inter-zone connections rules are satisfied. Table D.30 indicates that the rules are satisfied.

Table D.30 Inter-zone Data Flow Table

Inter-zone Data Flow Table							
Sending Zone			*Receiving Zone*			*Interconnection Device*	
ID	*Eval. Level*	*Processing Range*	*ID*	*Processing Range*	*Least Cleared User*	*Type*	*Eval. Level*
A	E4	U-C	B	U-S	C	Diode	E6
B	-	U-S	A	-	-	Integrity Filter	E5
B	E3	U-S	C	U-TS	TS(NV)	Diode	E6
C	-	U-TS	B	-	-	Integrity Filter	E6 (closed)

Note
Entries marked (-) are not applicable to the interconnection device type.

DISTRIBUTION

	Copy No.
Defence Science and Technology Organisation	
Chief Defence Scientist)	
Central Office Executive)	1
Counsellor, Defence Science, London	Cont Sht
Counsellor, Defence Science, Washington	Cont Sht
Scientific Adviser, Defence Central	1
Scientific Adviser, Defence Intelligence Organisation	1
Navy Scientific Adviser	1
Air Force Scientific Adviser	1
Scientific Adviser, Army	1
Electronics Research Laboratory	
Director	1
Chief, Communications Division	Cont Sht
Chief, Electronic Warfare Division	Cont Sht
Chief, Information Technology Division	1
Research Leader, Command and Control and Intelligence Systems	1
Research Leader, Human Computer Interaction	1
Head, Image Information Group	1
Head, Information Acquisition and Processing Group	1
Head, Information Management Group	1
Head, Command Support Systems Group	1
Head, Simulation and Assessment Group	1
Head, Exercise Analysis Group	1
Head, C^3I Systems Engineering Group	1
Head, Software Engineering Group	1
Head, Computer Systems Architecture Group	1
Head, Trusted Computer Systems Group	12
Dr. M. Anderson, Trusted Computer Systems Group	10
Publicity and Component Support Officer ITD	1
Media Services	1
Libraries and Information Services	
Australian Government Publishing Service	1
Defence Central Library, Technical Reports Centre	1
Manager, Document Exchange Centre, (for retention)	1
National Technical Information Service, United States	2
Defence Research Information Centre, United Kingdom	2
Director Scientific Information Services, Canada	1
Ministry of Defence, New Zealand	1
National Library of Australia	1
Defence Science and Technology Organisation Salisbury, Research Library	2

Library Defence Signals Directorate, Melbourne	1
British Library Document Supply Centre	1
Other Organisations	
Defence Signals Directorate	
Mr John Rogers	1
Dr Jeremy Dawson	1
Mr Tony Apted	1
Directorate of Communications and Information Systems - Army	
Maj Hans Willink	1
Defence Security Branch	
Mr Bill McCallum	1
Mr Colin Hale	1
Maj Simpson	1
DGJOP	
Brig E.F. Pfitzner	1
DCIS-A	
Col D.J. O'Neill	1
DCCP-A	
Col M.F. Collins	1
DNC4I	
Capt I.E. Pfennigwerth	1
DCIS-AF	
Gp Capt J.V. Tyrrell	1
DGCIS	
Air Cdre D.T. Bowden	1
DGJCE	
Air Cdre N.P. Middleton	1
DHIS	
Mr M.C. Peck	
Defence Intelligence Organisation	
PDADFDIS Capt. J.L. Raleigh	1
PRS-IDS (DIO) P. Drewer	1
Spares	
Defence Science and Technology Organisation Salisbury, Research Library	6

Department of Defence

DOCUMENT CONTROL DATA SHEET

Page Classification
UNCLASSIFIED
Privacy Marking/Caveat (of Document) N/A

1a. AR Number	1b. Establishment Number	2. Document Date	3. Task Number
AR-006-955	ERL-0621-RR	JUNE 1992	DEF 4B/VGJ

4. Title	5. Security Classification	6. No. of Pages	7. No. of Refs.
TECHNICAL RATIONALE FOR THE AUSTRALIAN COMPUTER SECURITY RISK ANALYSIS GUIDELINES	U (Document) U (Title) U (Abstract) S (Secret) C (Confi) R (Rest) U (Unclass) * For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.	128	22

8. Author(s)	9. Downgrading/Delimiting Instructions
J. Hellewell*, M. Anderson and B. Billard *Under contract from AWA Defence Industries	N/A

10a. Corporate Author and Address	11. Officer/Position responsible for
Electronics Research Laboratory PO Box 1600 SALISBURY SA 5108	Security.. Downgrading.. Approval for Release.........DERL........................
10b. Task Sponsor DSD	

12. Secondary Distribution of this Document

APPROVED FOR PUBLIC RELEASE

Any enquiries outside stated limitations should be referred through DSTIC, Defence Information Services, Department of Defence, Anzac Park West, Canberra, ACT 2600.

13a. Deliberate Announcement

No limitation

13b. Casual Announcement (for citation in other documents)

- [√] No Limitation
- [ ] Ref. by Author , Doc No. and date only.

14. DEFTEST Descriptors	15. DISCAT Subject Codes
Computer security, computer information security, Secure communications, Risk analysis	1208

16. Abstract

This document provides guidance to Australian Government agencies, both defence and civilian, on the specification and selection of trusted computing systems and products to be used for the electronic processing of National Security and/or Sensitive Material

Page Classification
UNCLASSIFIED

16. Abstract (CONT.)

17. Imprint

Electronics Research Laboratory
PO Box 1600
SALISBURY SA 5108

18. Document Series and Number	19. Cost Code	20. Type of Report and Period Covered
ERL-0621-RR	822522	RESEARCH REPORT

21. Computer Programs Used

22. Establishment File Reference(s)

23. Additional information (if required)